UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
FACULTAD DE INGENIERÍA
DIRECCIÓN DE POSTGRADO
PROGRAMA DE SISTEMAS DE INFORMACIÓN

TRABAJO DE GRADO DE MAESTRIA

MODELO DE EVALUACIÓN INTEGRAL DEL SISTEMA DE INFORMACIÓN ADMINISTRACIÓN DE RIESGO DE LEGITIMACIÓN DE CAPITALES EN LA BANCA PÚBLICA VENEZOLANA.

Presentado por
García Gil Juisgarlin Cecilia

Para optar al título de
Magíster en Sistemas de Información

Tutora
Guillén Guédez Ana Julia

Caracas, noviembre de 2017

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
FACULTAD DE INGENIERÍA
DIRECCIÓN DE POSTGRADO
PROGRAMA DE SISTEMAS DE INFORMACIÓN

TRABAJO DE GRADO DE MAESTRIA

MODELO DE EVALUACIÓN INTEGRAL DEL SISTEMA DE INFORMACIÓN ADMINISTRACIÓN DE RIESGO DE LEGITIMACIÓN DE CAPITALES EN LA BANCA PÚBLICA VENEZOLANA.

Presentado por
García Gil Juisgarlin Cecilia

Para optar al título de
Magíster en Sistemas de Información

Tutora
Guillén Guédez Ana Julia

Caracas, noviembre de 2017

Universidad Católica Andrés Bello
Vicerrectorado Académico
Facultad de Ingeniería
Dirección de Postgrado
Programa de Sistemas de Información

Atentamente: Prof. María Esther Remedios.

Referencia: Aprobación de Tutoría

Por la presente hago constar que he leído el borrador final de Trabajo de Grado de Maestría, presentado por la ciudadana **Juisgarlin Cecilia García Gil**, portadora de la Cédula de Identidad 18.032.829 para optar al Título Magíster en Sistemas de Información, cuyo título tentativo es: **Modelo de Evaluación Integral del Sistema de Información Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.**

En la ciudad de Caracas, al 06 día del mes de noviembre de 2017.

Guillén Guédez Ana Julia
C.I. V – 7.599.767

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
FACULTAD DE INGENIERÍA
DIRECCIÓN DE POSTGRADO
PROGRAMA DE SISTEMAS DE INFORMACIÓN

MODELO DE EVALUACIÓN INTEGRAL DEL SISTEMA DE INFORMACIÓN ADMINISTRACIÓN DE RIESGO DE LEGITIMACIÓN DE CAPITALES EN LA BANCA PÚBLICA VENEZOLANA

Autor: García Gil Juisgarlin Cecilia
Tutor: Guillén Guédez Ana Julia
Año: 2017

Resumen

Considerando la existencia de diversas actividades que exponen al sistema financiero venezolano a ser utilizado para la Legitimación de capitales, las entidades no solo necesitan destinar recursos para la creación y operación de áreas de cumplimiento normativo, sino cumplir con el marco regulatorio nacional, para evitar a la entidad multas, sanciones y posibles responsabilidades penales así como garantizar la reputación de la institución y proteger sus bienes y activos. Se requiere mejorar los procesos internos, con herramientas y técnicas que ayuden al control de actividades ilícitas. Se propone un proyecto de investigación cuyos objetivos son: plantear un modelo de evaluación integral del sistema de Administración de Legitimación de Capitales en la Banca Pública, diagnosticar el problema existente en el Sistema de Administración de Legitimación de Capitales, identificar los requerimientos en el negocio de la Banca Pública en Venezuela, formular un modelo de evaluación integral del sistema, y evaluar dicho modelo. Dichos objetivos fueron logrados basados con una investigación desarrollo, con diseño de campo no experimental y el instrumento que se utiliza para evaluar la propuesta será el juicio de experto, como resultado de lo antes escrito se propone un modelo de Evaluación Integral del Sistema de Legitimación de Capitales. De lo descrito anteriormente se concluye que este modelo permitirá la adecuada gestión y eficiencia en la prevención de Legitimación de Capitales en la banca pública.

Palabras Clave: Sistemas de Información, Banca Pública, Evaluación Integral, Administración de Riesgo, Legitimación de Capitales, Software Tecnología.

Línea de investigación: Ingeniería del Software.

INDICE GENERAL

Índice de figuras ix
Índice de tablas x
Lista de Acrónimos xi
Introducción 1

Capítulo I
Planteamiento del problema 5
Objetivos de la investigación 7
Objetivo general 7
Objetivo de la investigación 8
Justificación e importancia 8
Alcance 9

Capítulo II
Antecedentes de la investigación 10
Bases teóricas 17
Necesidad de información y conocimiento en la empresa 17
Las empresas en la era de la información 18
El valor de la información 19
Información que las empresas necesitan 21
Información estratégica 22
Información táctica 22
Información técnico operacional 22
Sistema de ayuda a la toma de decisiones 23
El entorno de la seguridad en el comercio electrónico 24
Dimensiones de la seguridad en el comercio electrónico 25
La integridad 26
La no repudiación 26
La autenticidad 26

La confidencialidad 26
La disponibilidad 27
Sistema financiero 27
Componentes del sistema financiero 27
Mercados financieros 28
Instituciones financieras 28
Instrumentos financieros 29
Sistemas de pago 29
Tipos de sistemas de pago 29
Efectivo 30
Transferencia de cheques 31
Tarjeta de crédito 31
Valor almacenado 32
Saldo acumulado 33
Habilitadores de comercio electrónico con tarjeta de crédito 34
Limitaciones de los sistemas de pago con tarjeta de crédito en línea 35
Carteras digitales 37
Sistemas de pagos de valor almacenado en línea 37
Sistema de pago de saldo acumulado digital 41
Sistemas de pago con cheques digitales 42
Sistemas de pago inalámbricos 43
Derechos de privacidad de información 44
Gobierno corporativo, gestión riesgo y cumplimiento de ley (GR&C) 46
¿Qué es el gobierno corporativo (Governance)? 47
¿Qué es gestión integral de riesgo, gir (entreprise risk management – erm)? 48
¿Qué es el cumplimiento de ley (compliance)? 50
Modelo integrado de gobierno corporativo, gir y cumplimiento de ley (GR&C) 51
Componentes de la GIR 57
Descripción general del riesgo operacional 60
Investigaciones financieras de orientación 63
Objetivos y beneficios de la investigación financiera 64

Bases legales 65
Constitución de la república bolivariana de venezuela 66
Grupo de acción financiera internacional (GAFI) 68
Comité de basilea 68
Superintendencia de las instituciones del sector bancario (SUDEBAN) 69
La organización internacional de entidades fiscalizadoras superiores (INTOSAI) 70
Normas internacionales de las entidades fiscalizadoras superiores (ISSAI) 71

Capítulo III
Tipo de investigación 72
Diseño de la investigación 72
Unidad de análisis 73
Procedimientos objetivos 74
Fases de la Investigación 75
Operacionalización de las variables 76
Consideraciones éticas y legales 78

Capítulo IV
Fundamentos organizacionales 79

Capítulo V
Analisis de brecha 88

Capítulo VI
Trazabilidad 105

Capítulo VII
Clasificación de los riesgos 107

Capítulo VIII
Aplicación de la prueba de concepto 122

Capítulo IX
Conclusiones y Recomendaciones 127

Referencias bibliográficas

INDICE DE FIGURAS

Figura		Página
1	Entorno de seguridad en el comercio electrónico	25
2	Esquema general tarjeta inteligente mondex	40
3	Tarjeta octopus	41
4	Modelo integrado de gobierno corporativo, gestión de riesgo y cumplimiento de ley (GR&C)	52
5	Legitimación de Capitales	85
6	Legitimación de Capitales y entes externos	104
7	Tipología de riesgo	108
8	Clasificación de los riesgos	109
9	Cliente servidor Banca Pública Venezolana	110
10	Arquitectura banco pequeño para legitimación de capitales	113
11	Arquitectura general para el modelo	114
12	Entidad relación para el modelo propuesto	115
13	Core banca pública	116
14	Prototipo dashboard alarmas	117
15	Prototipo Dashboards alarmas por cliente	118
16	Prototipo Dashboards alarmas	118
17	Prototipo Dashboards zonas riesgo	119
18	Caso generar alerta 5	124
19	Caso solicito ente gubernamental	125
21	Caso de auditoria	126

INDICE DE TABLAS

Tabla		Página
1	Instituciones financieras del estado venezolano	28
2	Dimensiones de los sistemas de pago	34
3	Criterios para un programa efectivo de cumplimiento de ley	54
4	Roles y responsabilidades bajo un modelo GR&C	56
5	Bases legales de la investigación	66
6	Operacionalización de las variables de la investigación	77
7	Banca pública venezolana	80
8	Análisis de brecha	89
9	Empresas de Software	119

LISTA DE ACRÓNIMOS

ALA: Antilavado de activos.

APNFD: Actividades y Profesiones No Financieras Designadas.

AUSTRAC: (Australian Transaction Reports and Analysis Centre) Centro de análisis e informes de transacciones australianas.

BCBS: (Basel Committee on Banking) Comité de Basilea sobre Banca.

BI: (Business Intelligence) Inteligencia de negocio.

DDC: Debida diligencia del cliente.

EUA: Estados Unidos de America.

FINCEN: (Financial Crimes Enforcement Network) Red de Ejecución de Delitos Financieros.

FT: Financiación al terrorismo.

GAFI: Grupo de Acción Financiera Internacional.

GIR: Gestión Integral de Riesgo.

GR&C: (Governance, Risk and Compliace) Gobernanza, riesgo y cumplimiento.

INTOSAI: Organización Internacional de Entidades Fiscalizadoras Superiores.

ISSAI: Normas Internacionales de las Entidades Fiscalizadoras Superiores.

LD: Lavado de dinero.

LOCDO: Ley Orgánica Contra la Delincuencia Organizada.

OAR: Organismo Autónomo de la Recaudación.

OFAC: Oficina para el Control de Activos Extranjeros.

ONA: Oficina Nacional Antidrogas.

SENIAT: Servicio Nacional Integrado de Administración Aduanera y Tributaria.

SUDEBAN: Superintendencia de las Instituciones del Sector Bancario de Venezuela.

UNIF: Unidad Nacional de Inteligencia Financiera.

INTRODUCCIÓN

La integración de América Latina, ha permitido el flujo comercial a gran escala entre los diferentes países, que influye en el rápido desarrollo de la tecnología tanto en la comunicación como en la información, dando paso a mecanismos más efectivos para realizar las negociaciones.

Dentro de este mundo de tecnología la herramienta más utilizada es internet, y entre los más beneficiados de dicho servicio se encuentran las instituciones financieras; ya que permiten mayor contacto del cliente y las instituciones a través de las transacciones de la red sin limitantes de distancias ni horarios. Aunque la herramienta sea de gran utilidad y tenga muchas ventajas, tiene su punto vulnerable ya que puede ser utilizado por los usuarios como medio para ingresar en el sistema económico mundial las ganancias provenientes de actividades ilícitas.

Actualmente, en Venezuela existen diversas actividades ilícitas asociadas a la corrupción, el narcotráfico, los secuestros, entre otros, que estarían utilizando las organizaciones financieras; para ingresar al sistema financiero, dinero obtenido de manera ilícita.

La Legitimación de Capitales, el Financiamiento del Terrorismo y demás delitos económicos, su importancia se remonta al final de la década de los ochenta cuando la comunidad internacional suscribió la Convención de Viena (1988) y se emitió la Declaración de Principios del Comité de Basilea (1988). Pero, sin embargo, actualmente en las instituciones financieras se ha observado un incremento significativo y acelerado de estas actividades ilícitas, ocasionando problemas

importantes al sistema financiero, lo cual es difícil de controlar, monitorear y rastrear con los métodos y procesos que actualmente tienen debido a la multiplicidad de transacciones y usuarios, la velocidad de cada transacción, los diversos lugares geográficos del cual procede, los montos bajos en múltiples transacciones, entre otros.

Es de vital importancia, para la organización proteger el nombre de la entidad financiera, debido a que el prestigio de una entidad financiera está en riesgo si es utilizada por las bandas delictivas para la legalización del dinero mal habido; sin embargo en Venezuela, se cuenta con la Superintendencia de Bancos (SUDEBAN), el cual es un ente, encargado de supervisar, controlar y vigilar a las instituciones financieras, con el fin de evitar o minimizar el riesgo presente en la banca, y cuidar el correcto y eficiente funcionamiento del Sistema Financiero Venezolano.

Las instituciones financieras deben cumplir con ciertas normativas legales que establece la Superintendencia de Bancos (SUDEBAN), para la prevención de la Legitimación de Capitales y Financiamiento al Terrorismo.

En este sentido, la banca pública Venezolana, y en pro del buen funcionamiento del Sistema Financiero en Venezuela y la razón de la presente investigación “Modelo de Evaluación Integral del Sistema de Información Administración de Riesgo de Legitimación de Capitales en la Banca Venezolana”, podrá ser utilizada como herramienta de evaluación, control y detección, dando un gran aporte y valor agregado al sistema financiero en Venezuela , para la mejor gestión en cuanto a la Legitimación de Capitales se trata.

Este proyecto de investigación consta de ocho (8) capítulos:

Capítulo I. Propuesta de Investigación, contentivo del planteamiento de la situación, los objetivos de la investigación, su justificación, alcances y limitaciones.

Capítulo II. Marco Teórico, conformado con los antecedentes y las bases teóricas que respaldan el marco conceptual de la investigación.

El Capítulo III. Marco Metodológico, se refiere a la metodología aplicada para llevarla a cabo y desarrollarla, las técnicas de recolección de la información, consideraciones éticas y legales, aspectos administrativos y financieros así como el cronograma de actividades, en el cual se expresan los recursos y el tiempo necesario para la ejecución de la investigación.

El Capítulo IV. Marco Organizacional, contiene información referente a los bancos pertenecientes a la banca pública, marco referencial de los bancos pertenecientes a la banca pública, fundamento de los bancos pertenecientes a la banca pública, visión y misión de la banca pública.

El Capítulo V. **Identificación de los requerimientos técnicos y funcionales de un sistema de Administración de Riesgo de Legitimación de Capitales en la banca pública venezolana**, contiene información sobre las leyes vigentes en la banca pública venezolana, el análisis de brecha donde se especifica los requerimientos exigidos por el GAFI, la situación actual en la banca venezolana y el escenario ideal basándose en las mejores prácticas internacionales.

El Capítulo VI. **Evaluación del nivel de brecha de los requerimientos de trazabilidad en el Sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Venezolana**, contiene la evaluación de brecha y la ampliación de la afectación de la legitimación de capitales más allá de la banca pública, involucrando a entidades públicas que se encargan del control de tributos, de igual manera tomando en cuenta la ISO 9001:2008 se observó la trazabilidad y los componentes necesarios.

El Capítulo VII. **Formular un modelo de evaluación integral del sistema de Administración de Riesgo de Legitimación de Capitales en el caso de estudio,**

se refiere a los riesgos asociados al modelo, el tipo de arquitectura que se empleara para la implementación del modelo, las estrategias, y la tecnología empleada para el modelo, así como también se mencionan las compañías más reconocidas en cuanto a soluciones tecnológicas se trate.

El Capítulo VIII. **Aplicación de una prueba de concepto del modelo de evaluación integral del sistema Información Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana**, contiene los casos de pruebas para valorar el concepto antes del inicio del desarrollo.

El Capítulo IX. Conclusiones y Recomendaciones, se muestra las conclusiones de la investigación en orden con relación a cada objetivo específico. De igual manera se plantea una recomendación general. Al final del mismo las referencias bibliográficas, que permiten identificar las publicaciones citadas y fuentes consultadas en la presente investigación.

Al final del mismo las referencias bibliográficas, que permiten identificar las publicaciones citadas y fuentes consultadas en la presente investigación.

CAPÍTULO I. PROPUESTA DE INVESTIGACIÓN

PLANTEAMIENTO DEL PROBLEMA

Desde el siglo pasado, a mediados de la época de los ochenta, la lucha contra el tráfico de drogas y contra otras actividades como lo es el blanqueo de capitales, ha aumentado progresivamente, aunque no es solo combatirlos sino además, para prevenir y perseguir. El fenómeno del blanqueo de capitales generó una gran preocupación en el ámbito internacional fundamentalmente por el carácter no público, semiprivado de las organizaciones que dan los primeros pasos, las diversas limitantes en la lucha contra el blanqueo de capitales procedentes del narcotráfico y al uso de las entidades bancarias para hacer parecer el dinero ilícito como licito.

La lucha contra la legitimación de capitales sólo es eficaz si los servicios encargados de combatirlo tienen acceso a la información de las transacciones financieras y los movimientos internacionales de fondos y capitales en todas sus modalidades. Desde finales del decenio 1980, la mayoría de los Estados que han aprobado una legislación sobre legitimación de capitales, han establecido un sistema que permite a las instituciones financieras comunicar a las autoridades ciertas operaciones bancarias y, en particular, toda operación que pueda encubrir en forma evidente o sospechosa, actos de legitimación de capitales que incluso muchas a veces obligan a la banca a hacerlo.

El tipo de declaraciones que deberán presentar esos organismos depende de la legislación vigente. Podrá consistir en una declaración sistemática de ciertas operaciones, incluso no sospechosas, como la transferencia de dinero en efectivo, o en una declaración tan sólo de las operaciones cuyo contexto permita sospechar un movimiento de dinero mal habido al banquero u operador. En todos estos casos, esta declaración deberá "procesarse", a fin de determinar con precisión si se trata de un caso de legitimación de capitales, para lograr la posterior detención de los autores y el decomiso de los bienes de origen delictivo.

El sistema financiero Venezolano presenta diversos riesgos que exponen a sus instituciones a ser utilizadas para la Legitimación de Capitales, por las deficiencias estratégicas en materia de prevención, control, fiscalización y penalización de los graves delitos de lavado de dinero actividad que consiste en darle apariencia de legitimidad al dinero proveniente de actividades ilícitas, y financiamiento al terrorismo que consiste en un acto de proporcionar apoyo económico a las organizaciones o individuos que tienen como propósito la comisión de acciones de naturaleza terrorista. Por tal motivo, se debe fortificar y actualizar los mecanismos de prevención y administración, mejorando los procedimientos internos, con herramientas y técnicas que ayuden al control de actividades ilícitas.

Para esto es necesario la utilización de teorías, métodos y herramientas teniendo en cuenta las restricciones financieras, organizacionales, técnicas en cuanto a producción de software y técnicas usadas en transacciones internacionales, guiadas por recomendaciones internacionales para afrontar los riesgos (Basilea II y Basilea III).

Las organizaciones tienen que aceptar y manejar los cambios de la tecnología de la información ya que estos cada vez se producen rápidamente.

La banca pública por estar comprometida con el estado venezolano debe ser capaz de evaluar los requerimientos mínimos exigidos por las ley, ajustarlos y fortalecerlos de acuerdo con las actividades cambiantes de su negocio y como parte de su responsabilidad, con el fin de lograr una eficiente y adecuada gestión de prevención de los riesgos de legitimación de capitales y financiamiento al terrorismo.

Todo el planteamiento anterior conduce a formular la siguiente interrogante de la investigación:
¿Cómo desarrollar un modelo de evaluación integral del sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Pública, ayudará a la

problemática existente en la gestión de prevención de los riesgos de legitimación de capitales y financiamiento al terrorismo?

Sistematización de la Investigación:

¿Cuáles deben ser las herramientas y estrategias necesarias que deben ser tomadas en cuenta para el sistema de administración integral de legitimación de capitales con el fin de controlar y prevenir la legitimación de capitales a través de la banca?

¿Cuáles son los niveles de trazabilidad de legitimación de capitales en el negocio de Banca Pública Venezolana?

¿Cuáles son los elementos para la formulación de un modelo de evaluación integral del sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Pública, ayudará a la problemática existente?

¿Cuál es el resultado de evaluar el modelo propuesto del sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Pública?

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo General.

Desarrollar un Modelo de Evaluación Integral del Sistema de Información Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.

Objetivos Específicos.

1. Identificar los requerimientos técnicos y funcionales de un sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.

2. Evaluar el nivel de brecha de los requerimientos de trazabilidad en el Sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.

3. Formular un modelo de evaluación integral del sistema de Administración de Riesgo de Legitimación de Capitales en el caso de estudio.

4. Aplicar una prueba de concepto del modelo de evaluación integral del sistema Información Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.

JUSTIFICACIÓN E IMPORTANCIA

El problema planteado busca satisfacer una necesidad que surge en el sector financiero y por lo tanto afecta la economía en Venezuela, invadiendo el mercado financiero con capitales de procedencia dudosa o incierta, esta actividad provienen de unidades muy bien organizadas que poseen gran poder económico, tecnológico e influencias en todos los estratos políticos y sociales, es un problema mundial que afectando a las naciones.

Se propone un modelo de evaluación integral que ayude al área de Legitimación de Capitales y Financiamiento al Terrorismo a la mejor gestión de la unidad permitiendo un control preventivo y curativo para el saneamiento y mantenimiento de los esquemas financieros y valores económicos, cumpliendo con los lineamientos solicitados por el ente regulador Superintendencia de Bancos (SUDEBAN); por ello será necesario evaluar los requerimientos mínimos exigidos por Superintendencia

de Bancos (SUDEBAN), el negocio de la organización y sus procesos. La línea de investigación Ingeniería de Software.

ALCANCE

El proyecto en cuestión se encuentra delimitado en un primer plano al contexto nacional, dentro del territorio geográfico y fronteras políticas de Venezuela. Esta investigación permitirá explorar y ayudará a la banca a la mejor gestión de prevención en cuanto a legitimación de capitales basado con la normativa legal vigente en el país.

Además permitirá servir como base para otros estudios, que tengan como punto de partida la problemática aquí especificada. El alcance de este proyecto es proponer un modelo y quedará por parte de las instituciones que desee implantarla.

CAPÍTULO II. MARCO TEÓRICO

Los fundamentos teóricos sirven de base para conceptualizar el desarrollo de una investigación, para esto es necesario consultar diferentes fuentes primarias y secundarias con el fin de recopilar conceptos que permitan entender y observar los fundamento para el desarrollo de un modelo de evaluación de Legitimación Capitales.

ANTECEDENTES DE LA INVESTIGACIÓN

En esta sección se presentan artículos y tesis de grado relacionados con el problema de investigación planteado, lo que permitirá precisar y delimitar el objeto de estudio y por consiguiente los propósitos de la investigación.

Según Guevara (2015), en su trabajo de Grado presentado en la Universidad de Carabobo, para obtener el título de Magister en Administración de Empresas Mención Finanzas, titulado: “La Legitimación de Capitales en el Sistema Financiero Venezolano”

Indica la importancia que tiene para el Sistema financiero venezolano el control en los clientes y las transacciones por cada cliente, el tema central basado en el marco de un sistema bancario con debilidades en el orden jurídico. Detalla los riesgos implícitos asociados a la legitimación de capitales y los entes gubernamentales que participan en este proceso de prevención, control y fiscalización de acuerdo a las leyes venezolanas.

Identifica 5 tipos de riesgos asociados a la legitimación de capitales: reputacional, legal, operacional, de contagio y transnacional, causando efectos perjudiales tanto en a la entidad bancaria como a la economía del país, pérdida de credibilidad, violaciones de normas, mal uso del cliente, acciones relacionadas asociados, imposibilidad de detener una ilegitima, entre otras.

Según Lopez y D'Antoni (2014) en su artículo titulado "The Modern Data Warehouse -How Big Data Impacts Analytics Architecture" expresan que las bases de datos no pueden verse como relacionales y no relacionales, deben ver más alla aprovechar al máximo las arquitecturas, buscando reducción de costo y tiempo. Ellos describen una tecnología llamada Hadoop que en sus inicios su fin era, un motor de búsqueda y procesador de datos en Yahoo, y con el tiempo se convirtió en una moderna arquitectura de análisis de datos, aunque en un principio fue un reto para la tecnología de información la implementación de Hadoop, inclusive se presentaron varias limitantes, más adelante se logró escalar para convertirse en un marco para el procesamiento de datos y un sistema de archivos distribuidos, esta combinación permitió llevar varias actividades simultáneamente, además la gran ventaja que se presentaba tolerancia a fallos durante la ejecución en el hardware de los productos básicos.

Según Gadda y Dey (2014) en su artículo titulado "Business Intelligence for Public Sector Banks in India: A Case study - Design, Development and Deployment" indican que a nivel mundial los bancos miden las siguientes caracteristicas: desempeño, rentabilidad, análisis, gestión riesgo, análisis histórico, tableros ejecutivos, informes normativos y la gestión de la relaciones con los clientes. La inteligencia de negocio es el siguiente paso lógico en los bancos de la india y en especial en el sector público, en la india varios bancos estan utilizando las soluciones de tecnología de información, con el fin de mejorar la eficiencia y competitividad del sector bancario mediante el fortalecimiento de los procesos administrativos internos y mejorar los procesos externos ofrecidos al cliente, ayudando así al cliente a la disminución de los costos.

Actualmente los organismos públicos de la india requieren afrontar un gran desafío en tener entre sus caracteristicas la aplicación de tecnología de punta, innovación, gestión e implementación de basilea II. En su artículo hacen especial énfasis que para cumplir todos los requisitos de basilea II, requieren tener una robusta y confiable arquitectura de inteligencia de negocio.

Según Kumar (2013), en su trabajo de grado presentado en la Universidad San Diego State, para obtener el título de magister of Science in Computer Science, titulado: “DATA ANALYSIS USING BUSINESS INTELLIGENCE TOOL”, manifiesta que día a día va creciendo la necesidad de las organizaciones de gestionar la información, ya que esta se va incrementado rápidamente y se necesita controlarla y utilizarla, la tecnología inteligencia de negocio se usa para gestionar , exportar y presentar los datos con el fin de trabajarlos y obtener de esa data el máximo para utilizarla en las decisiones del negocio, con el fin de apoyarse en estas herramientas y obtener el máximo provecho de la data, el objetivo fuerte es obtener data de otros procesos y por esta razón esta data debe tener la mayor calidad posible en la información suministrada.

En el artículo de Abzaltynova y Williams (2013), titulado “DEVELOPMENTS IN BUSINESS INTELLIGENCE SOFTWARE” presentan que la amplia gama de desarolladores han sido afectados por la economia, debido a la gran competencia que se tiene en el mercado, por tal motivo tienen que analizar que esta sucendiendo y buscar respuestas rapidas de como mejorar para ser cada dia mas competitivos y no pierdan clientes, entonces cada dia deben desarrollar con mayor rapidez y obteniendo productos de calidad a un precio muy bajo con el fin de mantener sus clientes, en la investigacion tomaron varias fases para la evaluacion de empresas importante, en cada fase se fueron observando las fortalezas y debilidades de cada empresa, los que eren muy buenos en la fase de analisis resultaban deficientes en la recopilacion de datos.

Toda compania por mas pequena que sea trata de introducir mejoras para ofrecer un software accesible, rapido, flexible con el fin que se administren cantidades creciente de datos, para persistir en el mercado y la compania a la cual le prestan el servicio esten bien informada al momento de tomar decisiones.

Según Mohammed (2010), en su trabajo de grado presentado en la Universidad Bradford, para obtener el título de Doctor Of Philosophy, Department of Computing, titulado: “PHISHING WEBSITE DETECTION USING INTELLIGENT DATA MINING TECHNIQUES”, expresa que los servicios ofrecidos a través de la banca online es uno de los más afectados en cuanto ataques informáticos, debido a la alto número de transacciones y la gran cantidad de dinero que se puede aprovechar en esta manera de estafa a través de la web, ya que suplantan identidad de empresas, con el fin que la persona estafada consiga ser engañada y acceda a dar la información para ingresar a sus cuentas bancarias, sin darse cuenta.

Además a través de estos sitios web se puede hacer uso de dinero ilegitimo, contratando a personas y ofreciéndole dinero fácil trabajando desde su casa, usando a estas personas para incorporar dinero producto de actividades ilícitas.

El autor plantea la importancia de detección de phishing con el fin de enfrentar las importantes pérdidas a nivel monetario y recuperar la confianza en los servicios basados en internet, el principal objetivo del tema de investigación del autor anteriormente citado es detectar sitios web fraudulentos usados como phishing en la banca electrónica.

Ramírez (2005), en su Trabajo de Grado presentado en la Universidad de Nueva Esparta, para obtener el título de Magister Scientiarum, titulado: “Estudio y Propuesta para Implantar una Unidad de Inteligencia Financiera en Venezuela”, cuyo objetivo general: Establecer y generar las recomendaciones con relación a cuáles serían los mejores mecanismos que deberían utilizarse para instalar y poner en operación la Unidad de Inteligencia Financiera en Venezuela.

Presenta que frente a la gravedad en cuanto el asunto del enriquecimiento ilícito, puede ser mejorado a través de un producto viable, factible y de gran utilidad que no solo repercute en el área tecnológica sino en la necesidad del cliente por mantenerse actualizado y conservar su competitividad, sin que esto implique

grandes gastos a nivel económico, también indica que no solo la voluntad contra el blanqueo de capitales es suficiente, es necesario tener herramientas que ayuden en esta lucha ya que el más fuerte tecnológicamente es el que sobrevive siempre y cuando tenga claro: las leyes, y los factores propios de cada país. Y como conclusión presenta que la tecnología de la información es la llave del triunfo y la gerencia tecnológica la mano que ejecuta.

En el artículo de Luciani (2006), titulado “La triple vertiente del riesgo de legitimación de capitales” indica que el riesgo operacional muchas veces es ocasionado a través de los procesos inadecuados en los sistemas internos de las entidades financieras, ya sea ocasionado por el personal o los software que poseen dichas instituciones.

Además hace referencia que aunque no hay manera de garantizar que no se realice a través de los bancos el blanqueo de capitales, las mejoras en los sistemas es de gran ayuda ya que más que un riesgo a nivel de las operaciones bancarias, causa grandes problemas en el activo más importante que tiene una institución financiera tal como lo es la confianza que tienen los clientes en la entidad financiera y en el buen nombre de la institución.

En varios países del mundo han elaborados normas sobre la administración de riesgos bancarios y en Venezuela a través de la Superintendencia de Bancos y Otras Instituciones Financieras han promulgado normas que ayuden a minimizar este riesgo presente en las instituciones bancarias en Venezuela. Todo esto ha despertado gran interés en las gerencias de riesgos de las distintas entidades financieras ya que trabajando en conjunto con la unidad de Legitimación de Capitales con el fin de medir y controlar todo aquel proceso que represente un riesgo para la institución.

El artículo de Pons (2010), titulado “Comentarios al Proyecto de Ley de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo: Nuevas Obligaciones para Entidades Financieras y otros Sujetos Obligados”. En su artículo hace un

análisis legal en el Proyecto de Ley de prevención del blanqueo de capitales y del financiamiento al terrorismo en España, donde a través de la ley pretende reforzar las medidas de control y supervisión del sistema financiero en España, adicionalmente explica que este proyecto de ley adapta las normativas internacionales que están mucho más estudiadas e informadas en cuanto a materia de prevención del blanqueo de capitales y la lucha contra el financiamiento al terrorismo incorporando nuevos deberes y principios de valoración del riesgo obligando a las entidades financieras a redefinir herramientas y procedimientos internos.

Como conclusión presenta que es bastante grave la situación presentada en cuanto a este delito y que el fin de todas estas leyes es la represión del producto y finalizar la delincuencia, fortaleciendo la protección del sistema financiero, y que aunque muchos entes no valoren o no tengan el conocimiento de lo grave de la situación a esta actividad hay que otorgarle prioridad.

Según Martínez y Coronado (2003), en su artículo “Indicadores para la Evaluación Integral de la Productividad Académica en la Educación Superior” expresan que a través de un sistema evaluativo que combinado con las principales áreas activas en una universidad con juicios valorativos, les permitió analizar e interpretar cada dato recopilado para emitir criterios de valor y recomendaciones de una forma integral, confirmando que si los datos obtenidos en cualquier evaluación son vistos aisladamente, su valor no se aprecia con toda claridad, pero al relacionarlos permite hacer comparaciones y observar los resultados con distintas panorámica.

Todo el sistema integrado de indicadores permite la posibilidad de hacer comparaciones con la modalidad integral con el fin que la compañía evaluada pueda seguir promoviendo e induciendo los procesos internos con un punto de vista distinto en comparación a otras compañías, ayudando a detectar los niveles deficientes en ciertas áreas que requieran ser fortalecidas para aumentar la calidad.

De igual manera permitirá detectar áreas de oportunidad que ha simple vistas no son detectadas.

Mejía (2008), en el artículo sobre “Fundamentación de un Sistema de Evaluación a la Gestión Integral de los Procesos Universitarios, sobre la Base de la Auditoría como Proceso, para la Universidad Católica de Oriente” expresa que las actividades de gestión se realizan de una manera establecida, de manera informal o formal y en conformidad con normas, procedimientos o rutinas de trabajo existentes. Los esquemas de trabajo están fijados de un modo concreto, y en hoy en día se siguen manteniendo.

Por esa razón se requiere disponer de un buen diagnóstico acompañado de un plan de acción y es necesario considerar una serie de aspectos claves que en muchas ocasiones pasan desapercibidos o equivocadamente se suponen. La evaluación integral de los procesos universitarios permitirá evidenciar la pertinencia en lo formativo y social, la eficiencia y efectividad de los mismos, asegurando el control de la institución por parte de la alta dirección con miras a la consecución del desarrollo sostenible y la creación de ventajas diferenciadoras en el sector educativo de nivel superior.

Los artículos y trabajos de grados mencionados anteriormente contribuyen en la fase inicial para el desarrollo de este trabajo ya que se requiere conocer sobre las bases legales de la investigación, los artículos de Luciani (2006) y Pons (2010), son de gran apoyo para el tema de investigación ya que es de gran apoyo ver las bases legales en cuanto a legitimación de capitales se trata y la gran controversia que se presenta a nivel nacional e internacional.

La legitimación de capitales aunque suele verse un tema netamente financiero necesita herramientas tecnológicas para luchar contra estas operaciones y transacciones financieras, ya que estos capitales ficticios afectan significativamente la estabilidad económica de la nación, hay que entender que no es posible combatir

a los grupos mafiosos e ilegales sin las herramientas tecnológicas adecuadas, para lo cual se hace necesario ser tan rápidos y si es posible más rápidos en el manejo de la información que la velocidad con que se mueven los grupos ilícitos en los procesos de legitimación de capitales, una excelente referencia sería el trabajo de grado de Ramírez (2005).

El establecimiento de estructuras contra la legitimación de Capitales a nivel de los Estados es datan de 1988, los primeros textos internacionales. En Europa desde el 10 de junio de1991, se obliga a declarar las operaciones sospechosas, de igual forma que en los Estados Unidos con organizaciones como la red de represión de delitos financieros (FINCEN), del departamento del tesoro de los Estados Unidos y Canadá con el centro australiano de análisis e informes sobre transacciones (AUSTRAC). En Europa, la obligación de declarar operaciones sospechosas .legislaciones nacionales. En el momento en que la mayoría de los países occidentales han establecido mecanismos de represión, es instructivo analizar cuáles son las opciones que se han aplicado para organizar y estructurar el procesamiento de la información sobre la actividad de legitimación de capitales.

BASES TEÓRICAS

Necesidad de Información y Conocimiento en la Empresa

Según Bitam (2011), las empresas actualmente caracterizan a la información como uno de los activos de la empresa, es así que se comienza a tratarla, especialmente aquella relacionada con datos para tomar decisiones, de una manera más metodológica. A continuación se exponen brevemente algunos conceptos relacionados con la información y su importancia estratégica para la toma de decisiones en las empresas.

Las Empresas en la Era de la Información

Desde que las organizaciones comenzaron a guardar los datos de sus operaciones en medios de almacenamiento físico, con el fin de permitirles una mayor administración y control de la información, ha existido una necesidad de utilizarla para atender las necesidades propias del negocio.

La información y su importancia estratégica comenzó a surgir cuando la competencia se hizo muy fuerte, y cada vez más y más productos similares, de diferentes compañías, se ponían a la venta, en ese momento el consumidor tuvo la opción de seleccionar aquello que más le conviniera o lo que más se adecuara a sus gustos y preferencias. Surge entonces la necesidad de brindar servicios adicionales para obtener la lealtad de los clientes, quienes poco a poco comenzaron a ver, no solo el producto que compraban, sino cómo eran atendidos, qué garantías se ofrecían sobre su compra, qué ventajas habría entre diferentes productos y, en general, evaluar todo lo que genera la diferenciación entre las compras que realizan. Cuando las empresas no tienen garantizada la venta de lo que producen, realizan un cambio paulatino hacia obtener de los datos toda la Marco Conceptual información útil y estratégica para mantenerse en el mercado, dándole un lugar preponderante al cliente.

Actualmente, se le da un peso específico muy importante a la información como el principal conocimiento que sostiene el negocio. Existen empresas que, de modo predominante, ofrecen servicios y giran su negocio principal sobre el manejo de la información (bancos, seguradoras, casas de bolsa, internet, etc.), en ellas es fácil identificar la importancia de la información, si no existiera ésta dejarían de existir.

Sin embargo, hay otras en las que su giro principal es alrededor de la producción, en ellas la información debe identificarse para analizar y perfeccionar su producción (porcentajes de desecho, líneas de producción, distribución de materias, suministro, inventarios y almacenes, procesos internos, publicidad y mercadotecnia, preferencias del cliente, etc.). De hecho, en cualquier empresa se está tratando de convertir, por todos los medios posibles, esa información en conocimiento que

mejore los procesos y, a su vez, se traduzca en ventajas competitivas en los mercados.

La idea de las empresas sedientas de información no surge de súbito, en realidad desde que se almacenan los datos debe entenderse que tendrían un fin utilitario en algún momento, caso contrario, cualquier dato de control sería desechado instantáneamente. Lo que si surge de súbito es la imprescindible necesidad de dar respuesta rápida a los requerimientos de información para la toma de decisiones para ayudar a mejorar de alguna manera los procesos internos de negocio.

El Valor de la Información

En la época actual, que se caracteriza por un crecimiento exponencial de las nuevas tecnologías de la información y las telecomunicaciones, los activos más valiosos de una empresa ya no son activos tangibles o los depósitos en los bancos, sino los conocimientos, habilidades, valores y actitudes de las personas que forman parte de una empresa. De hecho, para generar riqueza es suficiente tener conocimiento sobre un tema determinado y explotarlo de la mejor manera posible. Los factores de la producción como capital, tierra y trabajo, han sido sustituidos por el capital intelectual, que comprende todos aquellos conocimientos tácitos o explícitos que generan valor económico para la empresa.

Prácticamente nadie cuestiona el hecho de que de la actual Era de la Información y la información tiene un valor concreto en pesos, esto se evidencia porque existen empresas cuyo único negocio es alrededor de la venta de información, como por ejemplo Gartner Group, Empresas de Internet Amazon, entre otras.

Para identificar el valor concreto de la información en la organización se pueden realizar dos evaluaciones según Bitam (2011):

a- Todas las corporaciones tienen un modelo del mundo de negocios basado en la información que poseen, por ejemplo: ¿qué influencia la compra y la demanda?, ¿en dónde hay oportunidades de negocio?, ¿qué es lo que mueve la calidad del producto y la demanda de los clientes? A medida que esta información se vuelve más exacta, la capacidad de la empresa para competir se incrementa.

Visto así, la información corporativa es claramente un activo de la empresa que genera valor y su inexistencia genera "desvalor", o sea, pérdidas en caso de que existiera la información y ésta desapareciera, o bien, "no ganancias" en caso de que no exista.

b- Otra forma de entender la información como dinero es mediante su transformación en conocimiento tácito o explícito. El conocimiento tácito es el que tienen las personas producto de la experiencia, los estudios y la educación; los conocimientos explícitos son los que se almacenan en medios magnéticos como cintas y disquetes.

Información que las Empresas Necesitan

La tendencia de las organizaciones actuales es demandar información en los niveles donde antes la administración se basaba en la intuición y el sentido común para tomar decisiones. A pesar de que en los niveles operativos siempre se ha demandado información, históricamente no ha existido restricción alguna para brindarla al usuario. Más bien los mercados dinámicos han obligado a las empresas para que la información estratégica sea puesta en las computadoras de los directivos, este comportamiento se ha generalizado principalmente motivado por la facilidad y utilidad de la información compartida. En estos momentos la información fluye en todos los niveles de la organización con diferentes fines (comunicación, control, administración, evaluación, etc.) independientemente de los puestos. Las empresas están entendiendo que los niveles directivos tienen una gran responsabilidad al tomar decisiones, pues el impacto que generan recae sobre toda la organización, pero también existen más personas que toman decisiones y, a pesar de que éstas no tienen un impacto global, deben ser también correctas y oportunas, pues ciertos grupos dependen de las mismas.

Directores, gerentes, supervisores, jefes, todos aquellos que toman decisiones deben tener suficiente información para apoyarse en su trabajo cotidiano, el lugar que ocupen en la pirámide organizacional se vuelve secundario cuando el enfoque es hacia el manejo de procesos y todos los puestos tienen cierta relación y dependencia entre sí.

De modo general en una pirámide organizacional, los requerimientos informativos se dividen en 3 partes: Información Estratégica, Información Táctica, Información Técnico Operacional.

Información Estratégica

Está orientada principalmente a soportar la Toma de Decisiones de las áreas directivas para alcanzar la misión empresarial. Se caracteriza porque son sistemas sin carga periódica de trabajo y sin gran cantidad de datos, sin embargo, la información que almacenan está relacionada a un aspecto cualitativo más que cuantitativo, que puede indicar como operará la empresa ahora y en el futuro, el enfoque es distinto, pero sobre todo es distinto su alcance. Se asocia este tipo de información a los ejecutivos de primer nivel de las empresas.

Un punto importante es que la información estratégica toma grandes cantidades de datos de áreas relacionadas y no se enfoca específicamente hacia una sola, de ahí que las decisiones que puedan ser tomadas impactan directamente sobre toda la organización.

Información Táctica

Información que soporta la coordinación de actividades y el plano operativo de la estrategia, es decir, se plantean opciones y caminos posibles para alcanzar la estrategia indicada por la dirección de la empresa. Se facilita la gestión independiente de la información por parte de los niveles intermedios de la organización. Este tipo de información es extraída específicamente de un área o departamento de la organización, por lo que su alcance es local y se asocia a gerencias o subdirecciones.

Información Técnico Operacional

Se refiere a las operaciones tradicionales que son efectuadas de modo rutinario en las empresas mediante la captura masiva de datos y Sistemas de Procesamiento Transaccional. Las tareas son cotidianas y soportan la actividad diaria de la empresa (contabilidad, facturación, almacén, presupuesto y otros sistemas

administrativos). Tradicionalmente se asocian a las Jefaturas o Coordinaciones operativas o de tercer nivel.

Sistema de ayuda a la toma de decisiones

Son sistemas interactivos basados en la computación con el objetivo de ayudar a los actores a la toma de decisiones utilizando para ello datos y modelos para identificar y resolver problemas y tomar decisiones. Según Bonczek, Holsapple y Whinston (1981), el sistema debe añadir/ayudar/asistir al actor que toma decisiones en la resolución de problemas sin estructura o semiestructurados el sistema debe poseer una facilidad interactiva para consultas, con un lenguaje de consultas que sea fácil de aprender y usar. La ayuda de DSS a los managers/actores de toma de decisiones usa y manipula datos, aplica controles y heurística, y construye y usa modelos matemáticos. Según Turban (2001), un DSS tiene 4 características básicas: DSS incorpora datos y modelos; están diseñados para asistir a los managers en los procesos de decisión en las tareas semiestructuradas o sin estructura; ellos soportan, más que reemplazar, el juicio de la gerencia, y sus objetivos es la mejora de le efectividad de las decisiones, no la eficiencia con la que las decisiones son hechas.

EL ENTORNO DE LA SEGURIDAD EN EL COMERCIO ELECTRÓNICO

¿Qué es una buena seguridad en el comercio electrónico?

En el mercado actual donde el internet es una herramienta muy fácil de usar y que a la vez se presenta grandes riesgo, cada vez que se entra en un mercado se arriesga, inclusive se puede perder la privacidad. El principal riesgo que se presenta es pagar y no obtener lo adquirido, o que el dinero se pierda mientras se esté realizando las transacciones.

Los comerciantes y consumidores del comercio electrónico se enfrentan a muchos de los riesgos presenten en el comercio tradicional pero lo cambiante es el entorno donde se desarrolla una transacción. Aunque robo es robo, ya sea tradicional o digital, de manera digital se ha tratado de tener menos riesgo debido a leyes políticas, procedimientos industriales, nueva tecnología, procedimientos organizacionales que promulgarían a la disminución de desfalco, actos delictivos, destrucción maliciosa entre otros.

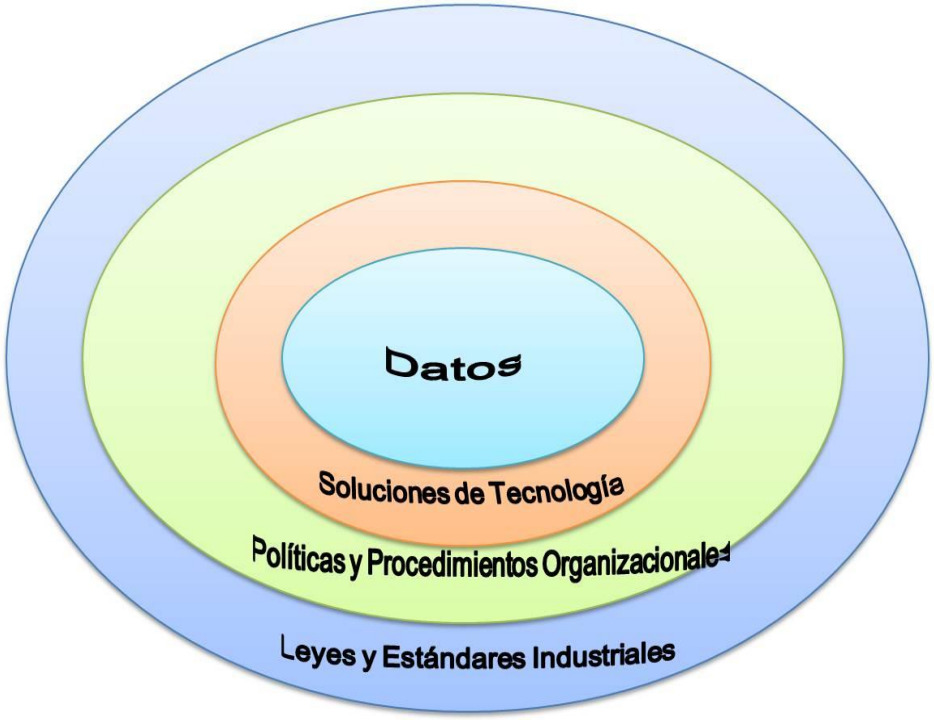

Figura 1. Entorno de Seguridad en el Comercio Electrónico.

Fuente: (Laudon K y Guercio C, 2006, p. 263)

En la figura 1 se muestra que la seguridad en el comercio electrónico, se va dando a varios niveles, por tal motivo se debe tomar en cuenta desde la nueva tecnología, pasando por las políticas y procedimientos organizacionales, y basándonos en las leyes y estándares industriales.

DIMENSIONES DE LA SEGURIDAD EN EL COMERCIO ELECTRÓNICO

Según Laudon y Guercio (2006) indican que existen seis dimensiones para la seguridad en el comercio electrónico y son las siguientes: integridad, no repudiación, autenticidad, confidencialidad, privacidad y disponibilidad.

La integridad

Es cerciorar y mantener la información contenida en un sitio web alejada y respaldada de personas no autorizadas que puedan manipular la información transmitida por internet o contenida en un sitio web, asegurando que la información que se muestra, sea la correcta.

La no repudiación

Asegurar que las personas que utilizan el comercio electrónico no desconozcan sus participaciones en línea. Ya que muchas veces se maneja un alias o seudónimo, conduciendo muchas veces a desconocer la realización de ciertas transacciones, inclusive al realizar pagos en línea con tarjetas de crédito ya que no existe una firma del cliente, el banco siempre estará de lado del cliente ya que el comerciante no tiene una prueba legal que certifique que el cliente solicitó la mercancía.

La autenticidad

Se refiere a la capacidad de identificar a la persona que se está conectando, para seguridad de los usuarios clientes y usuarios comerciantes, ya que se presentan casos de personas que pueden estar mintiendo sobre su identidad.

La confidencialidad

Se refiere a la capacidad que la información enviada o consultada solo este disponible para personas autorizadas a visualizar esa información. Debemos estar pendiente porque se confunde el término de confidencialidad con privacidad, la cual se refiere a la proporcionada por el cliente a un comerciante a través del comercio electrónico, un ejemplo muy claro de esto, es la preocupación de los comerciantes ya que ellos deben proteger la información y en el caso de que el sitio web sea hackeado no solo viola la confidencialidad de la persona, sino la privacidad.

La disponibilidad

Se refiere a la capacidad de asegurar que un sitio de comercio electrónico continúe funcionando como se espera.

La seguridad en el comercio electrónico está diseñada para proteger estas seis dimensiones. Cuando se compromete una de ellas, es una cuestión de seguridad.

SISTEMA FINANCIERO

Según Bello (2009), un sistema financiero es un conjunto de instituciones, mercados e instrumentos financieros, cuya misión conjunta fundamental es canalizar el ahorro financiero del país hacia los sectores productivos de la economía. El sistema financiero desempeña dicha función relacionando agentes económicos que desean invertir el excedente de sus ingresos sobre sus gastos, con otros agentes económicos que requieren esos recursos para financiar bienes de capital tal como adquisición de maquinarias, equipos, cubrir gastos de consumo con el fin de ayudar en la actividad productiva.

Componentes del Sistema Financiero

Según el actor anteriormente citado, los componentes del Sistema Financiero son los siguientes: mercados financieros, las instituciones financieras y los instrumentos financieros, el fin de estos componentes es intermediar o canalizar el ahorro en el país.

Mercados Financieros

Bello (2009), define los mercados financieros como un área geográfica en la cual mediante una serie de mecanismos se da conocer a los participantes de manera formal los precios de los diferentes activos financieros, con el fin de agilizar las transacciones de compra venta de dichos activos.

Instituciones Financieras

Las instituciones financieras incluyen las sociedades anónimas clasificadas en bancarias y no bancarias.

Instituciones Bancarias: Son aquellas instituciones cuyo fin es de atraer clientes para obtener como resultado el manejo de los fondos de personas naturales y jurídicas, conceder créditos, y vender titulo de valores.

Instituciones No Bancarias: Dentro de las instituciones bancarias se encuentran las compañías de seguros: las cuales son instituciones financieras no bancarias.

Las Entidades de inversión Colectiva: Se refiere a las instituciones que se encargan de encauzar los aportes de los inversionistas, cuyo principal objetico es un patrimonio común o construir un capital, integrado por una cartera de títulos valores u otros activos.

Entre las instituciones financieras del estado venezolano se encuentran:

Tabla 1. Instituciones financieras del estado venezolano

Banco de Venezuela	Banco Industrial de Venezuela
Banco del Tesoro	Banco Bicentenario
Banco de Fomento Regional de los Andes	Banco de Comercio Exterior
Banco de Desarrollo Económico y Social de Venezuela	Banco del Pueblo Soberano

Banco de Desarrollo de la Mujer	Corporación de Desarrollo de la Pequeña y Mediana Industria
Sociedad Nacional de Garantías Recíprocas para la Pequeña y la Mediana Industria	Fondo Nacional de Garantías Recíprocas para la Pequeña y la Mediana Industria
Fondo Nacional de Garantías Recíprocas para la Pequeña y Mediana Empresa	Fondo de Desarrollo Micro financiero
Fondo de Desarrollo Agropecuario, Pesquero, Forestal y Afines	Fondo de Crédito Industrial

Fuente: anuncios, 2014

Instrumentos Financieros

Los instrumentos financieros, llamados también activos financieros, están conformados por las obligaciones directas e indirectas generadas por los agentes económicos de gastos y las instituciones financieras no bancarias y bancarias. Algunos ejemplos son los bonos de la deuda pública y letras del tesoro emitidas por el Gobierno Nacional, papeles comerciales emitidos por sociedades anónimas no bancarias, entre otros.

SISTEMAS DE PAGO

Tipos de Sistemas de Pago

Según Laudon y Guercio (2006), indican que hay que estar familiarizado con los múltiples tipos de sistemas existentes para poder comprender todo el sistema de pago a través del comercio electrónico, ya que esto permitirá observar e identificar los requerimientos mínimos que deben de tener estos sistemas, y las nuevas ideas que pueden ir surgiendo en base a la nueva tecnología existente.

En la obra citada anteriormente indican que existen cinco tipos principales de medios de pago: Efectivo, Transferencia de Cheques, Tarjeta de Crédito, Valor Almacenado, Saldo Acumulado.

Efectivo

Moneda de curso legal definida por una autoridad nacional para representar un valor, en cantidades de transacciones es la forma más común de pago, el efectivo posee una característica clave debido a que puede cambiar de forma de valor sin intermediarios. Un ejemplo, las millas gratis de una aerolínea no son efectivo debido a que no se pueden convertir de inmediato en otras formas de valor; requieren la intermediación de un tercero (la aerolínea) para poder intercambiar por un valor (boleto de avión). Claro está algunas instituciones crean especies de efectivos privados conocido como vale, que se pueden cambiar de inmediato en las organizaciones participantes por artículos o efectivo.

La pregunta es ¿Por qué todavía tan popular el efectivo hoy en día?, unos de los puntos más relevantes es la portabilidad, proporciona un poder inmediato de realizar una compra, no requiere autentificación. El uso de efectivo es gratuito ya que al utilizar esta forma de pago no te cobran comisiones en el caso de realizar algún pago. El efectivo es anónimo y difícil de rastrear, y en ese sentido es “privado”. Otras formas de pago requieren un uso considerable de terceros y dejan un extenso rastro digital o de papel.

Por otra parte, el efectivo está limitado a transacciones más pequeñas, se roba fácilmente y no proporciona ninguna ganancia en el tiempo que transcurre la compra; además cuando se gasta desaparece, al realizar compras en efectivo muchas veces es irreversible a menos que exista un acuerdo previo con el vendedor.

Transferencia de Cheques

Se refiere a la transferencia de los fondos directamente a través de un cheque firmado de un consumidor a un comerciante y otra persona, según Laudon y Guercio (2006), es la segunda forma más común para realizar pago en EUA, luego del efectivo, en cuanto a término de número de transacciones, y la más común en términos del monto total gastado.

Aunque tiene algunas restricciones los cheques son utilizados para transacciones pequeñas y grandes, aunque muchas veces no se utilizan para pagos de pequeños montos, y en algunos comercios tienen ciertas restricciones debido al tiempo en que se tarda en liquidarse. Los cheques aunque son personalizados muchas veces se falsifican con más facilidad que el efectivo, además siempre requiere el trabajo de las instituciones financieras para que pueda llegar a terceros.

Tarjeta de Crédito

Según Espiñeira y asociados (2005), una tarjeta de crédito representa una cuenta que extiende crédito a los consumidores, a quienes permite comprar artículos difiriendo su pago, y realizar pagos a varios distribuidores al mismo tiempo. Las asociaciones de tarjetas de crédito como Visa y MasterCard son organizaciones sin fines de lucro que establecen los estándares para los bancos emisores (como Citibank) que emiten las tarjetas de crédito y procesan transacciones. Otras organizaciones (conocidas como centros de procesamiento o cámaras de compensación) son las que se encargan de la verificación de las cuentas y saldos. Los bancos emisores de tarjetas de crédito actúan como intermediarios financieros, minimizando el riesgo para las partes que participan en las transacciones.

Las tarjetas de crédito ofrecen a los consumidores una línea de crédito y la capacidad de realizar compras pequeñas y grandes al instante todo depende del límite. Son ampliamente aceptadas como una forma de pago, reducen el riesgo de

robo asociado con la portación de efectivo, e incrementan la conveniencia para el consumidor. Las tarjetas de crédito también ofrecen a los consumidores un periodo flotante considerable. Por ejemplo, con una tarjeta de crédito el cliente comúnmente no necesita pagar los artículos comprados sino hasta recibir una factura 30 días después. Los comerciantes se benefician del aumento en los gastos del consumidor que resultan del uso de las tarjetas de crédito, pero pagan una considerable cuota por transacción del 3 al 5 % del precio de compra a los bancos emisores. Además, en EUA la Regulación Z federal imponen los riesgos de la transacción (como el fraude de tarjeta de crédito, el repudio de la transacción o la falta de pago) en gran parte en el comerciante y el banco emisor de tarjeta de crédito. La Regulación Z limita la responsabilidad del tarjetahabiente por transacciones no autorizadas que ocurran antes de notificar al emisor de la tarjeta. Una vez que la tarjeta se reporta como robada, los consumidores no son responsables de los cargos subsiguientes.

Valor almacenado

Según Espiñeira y asociados (2005), las cuentas creadas al depositar fondos en una cuenta, y de la que se pagan o retiran fondos según se requiera, son sistemas de pago de valor almacenado. Estos sistemas son similares en ciertos aspectos a las transferencias de cheques (que también almacenan fondos), pero no implican la escritura de un cheque. Algunos ejemplos son las tarjetas de débito, los certificados de regalo, las tarjetas prepagadas y las tarjetas inteligentes. Las tarjetas de débito realizan un cargo inmediato en una cuenta de cheques u otra cuenta de demanda-depósito. Para muchos consumidores, el uso de una tarjeta de débito elimina la necesidad de escribir un cheque en papel. Hoy en día hay casi 300 millones de tarjetas de débito en uso a nivel naciones, y se utilizan en más de una cuarta parte de todas las compras hechas en tiendas de ventas al detalle estadounidenses. Sin embargo, y como las tarjetas de débito dependen de los fondos disponibles en la cuenta de banco de un consumidor, las compras más grandes por lo general se siguen realizando con tarjeta de crédito, y el uso de las tarjetas de débito en EUA

sigue siendo menor que en otras naciones desarrolladas, en parte debido a que no tienen la protección que ofrece la Regulación Z y no ofrecen un periodo flotante.

Saldo Acumulado

Las cuentas que acumulan gastos y para las que los consumidores hacen pagos periódicos son sistemas de pago de saldo acumulado. Según Espiñeira y asociados (2005), algunos ejemplos tradicionales son los servicios públicos, el teléfono y las cuentas de American Express, todos los cuales acumulan saldos, por lo general durante un periodo especificado (que casi siempre es un mes), y después reciben el pago completo al final del periodo.

En general, la mayoría de los consumidores utilizan efectivo, cheques y / o tarjetas de crédito. El sistema de pago especifico que se selecciones cambiará dependiendo de la situación de la transacción. Por ejemplo, se puede preferir el efectivo para mantener ciertas transacciones privadas y anónimas, pero el mismo consumidor tal vez quiera un registro de la transacción por la compra de automóvil.

Los comerciantes se interesan principalmente en mecanismos de pagos de bajo riesgo, bajo costo, irrefutables, seguros y confiables. En la actualidad, los comerciantes llevan gran parte del riesgo de los fraudes por cheques o tarjetas de crédito, la posibilidad de que rechacen los cargos y gran parte del costo del hardware para verificar los pagos. Comúnmente los comerciantes prefieren los pagos realizados en efectivo, cheque, y en menor grado con tarjeta de crédito, que por lo general acarrean cuotas altas y permiten que los clientes repudien las transacciones.

Tabla 2. Dimensiones de los Sistemas de Pago

DIMENSIONES DE LOS SISTEMAS DE PAGO					
DIMENSION	**EFECTIVO**	**CHEQUE PERSONAL**	**TARJETA DE CREDITO**	**TARJETA DE DEBITO**	**SALDO ACUM.**
Se puede convertir de inmediato, sin intermediario	si	no	no	no	no
Bajo costo en las transacciones pequeñas	sí	no	no	no	si
Bajo costo para las transacciones grandes	no	sí	sí	si	si
Costos bajos fijos para el comerciante	si	si	no	no	no
Refutable (se puede repudiar)	no	si	si	no (por lo común)	si
Riesgo financiero para el consumidor	si	no	hasta $250	limitado	no
Riesgo financiero para el comerciante	no	si	si	no	si
Anónimo para el consumidor	si	no	no	no	no
Anónimo para el comerciante	si	no	no	no	no
Se puede volver a gastar de inmediato	si	no	no	no	no
Seguridad contra el uso no autorizado	no	cierto grado	cierto grado	cierto grado	cierto grado
Resistente a alteraciones	si	no	si	si	si
Requiere autenticación	no	si	si	si	si
Se requiere Hardware especial	no	no	si; por el comerciante	si; por el comerciante	si; por el comerciante
El comprador mantiene un período flotante	no	si	si	no	si
Se requiere una cuenta	no	si	si	si	si
Tiene Valor monetario inmediato	si	no	no	si	no

Fuente: Adaptado de Mackie-Mason y White, 1996

Habilitadores de Comercio Electrónico con Tarjeta de Crédito

Las empresas que tienen una cuenta mercantil necesitan también comprar o construir un medio para manejar la transacción en línea; asegurar la cuenta mercantil es sólo el primer paso en un proceso de dos partes. Hoy en día, los proveedores de servicio de pagos de Internet pueden proveer una cuenta mercantil y las herramientas de software necesarias para procesar las compras en línea con tarjetas de crédito.

Por ejemplo, Authorize.net es un proveedor de servicio de pago por internet. Authorize.net ayuda a que un comerciante asegure una cuenta con uno de sus socios proveedores de cuentas mercantiles, y después proporciona el software de procesamiento de pagos para instalarlo en el servidor del comerciante. El software recolecta la información de las transacciones del sitio del comerciante y después la en ruta a través de la “puerta de enlace de pagos” de Authorize.net hacia el banco apropiado, asegurando que los clientes tengan autorización de realizar sus compras. Después, los fondos para la transacción se transfieren a la cuenta mercantil del comerciante.

Limitaciones de los Sistemas de Pago con Tarjeta de Crédito en Línea

Según Espiñeira y asociados (2005), hay varias limitaciones para el sistema de pagos con tarjeta de crédito. Las más importantes comprenden la seguridad, el riesgo del comerciante, el costo y la equidad social.

El sistema existente ofrece una mala seguridad. Ni el comerciante ni el consumidor se pueden autenticar por completo. El comerciante podría ser una organización designada para recolectar números de tarjeta de crédito, y el consumidor podría ser un ladrón que utilice tarjetas de crédito robadas o fraudulentas. El riesgo al que se enfrentan los comerciantes es alto: los consumidores pueden repudiar los cargos,

aun cuando se hayan enviado los artículos o se haya descargado el producto. La industria bancaria intentó desarrollar un protocolo de transacciones electrónicas seguro (SET) en 2000, pero este esfuerzo falló debido a que era demasiado complejo, tanto para los consumidores como para los comerciantes.

Los costos del crédito para los comerciantes también son considerables (aproximadamente 3.5% de la compra, más una cuota por transacción de 20 a 30 centavos, más otras cuotas de instalación). Los sistemas de valor almacenado como PayPal que dependen del sistema de tarjetas de crédito son aún más costosos: además de pagar la cuota de tarjetas de crédito del 3.5%, PayPal agrega una cuota variable de entre 1.5 y 3%, dependiendo del tamaño de la transacción. Los altos costos hacen que sea inconveniente vender artículos que cuestan menos de $10 en Web. La venta de artículos individuales, pistas de música o demás artículos pequeños no es muy factible con las tarjetas de crédito. Una manera de resolver este problema es acumular las compras de un consumidor durante un tiempo, antes de hacer el cargo a la tarjeta de crédito. Ésta es la táctica utilizada por la tienda de música *Apple iTunes*, que cobra 99 centavos por canción. En vez de cargar a la tarjeta de crédito del cliente cada canción individual, Apple acumula todas las compras que realice dentro de un período de 24 horas, para que se carguen a la cuenta de su tarjeta de crédito como un total por el período, y no como compras de canciones individuales. *iTunes* apenas si cubre los costos con una venta de 99 centavos, pero puede empezar a hacer dinero si el cliente compra varias canciones. En general, las empresas de crédito se oponen a la “acumulación”, ya que reduce sus ganancias.

Las tarjetas de crédito no son muy democráticas. Millones de adultos jóvenes no tienen tarjetas de crédito, junto con casi 100 millones de otros estadounidenses adultos, que no pueden costearse una tarjeta de crédito.

Carteras Digitales

Además de las tarjetas de crédito, también hay varias formas nuevas de pago que se han intentado, con éxito variado. Estas nuevas formas son las carteras digitales, el efectivo digital, los sistemas de pago de valor almacenado en línea, los sistemas de saldo acumulado digital y los sistemas de cheques digitales.

Una cartera digitalbusca emular la funcionalidad de la cartera que uno lleva consigo. Las funciones más importantes de una cartera digital son (a) autenticar al consumidor a través del uso de certificados digitales u otros métodos de cifrado, (b) almacenar y transferir un valor, y (c) asegurar el proceso de pago del consumidor al comerciante. Los primeros esfuerzos de muchas empresas no pudieron popularizar la idea de una cartera digital. Incluso Microsoft, que ofreció una cartera digital propietaria del lado del servidor, primero con Passport y después con MSN Wallet, abandonó en última instancia el esfuerzo en febrero de 2005. El esfuerzo más reciente por desarrollar algo parecido a una cartera digital es el servicio Checkout de Google, que es un sistema de procesamiento de pagos diseñado para hacer que el proceso de compras en línea sea más conveniente y sencillo. No almacena calor como PayPal, sino que comunica la información de tarjeta de crédito y personal de un comprador que sea necesaria para realizar una transacción con el comerciante. El comerciante recibe algunas garantías adicionales en la transacción con el comerciante. El comerciante recibe algunas garantías adicionales en la transacción de que el usuario ha sido autenticado por Google. No está claro aún qué tan exitoso puede ser este sistema.

Sistemas de Pagos de valor almacenado en línea

Los Sistemas de Pagos de valor almacenado en línea permiten a los consumidores realizar pagos instantáneos en línea a los comerciantes y a otras personas, con base en el valor almacenado en una cuenta en línea.

Paypal (comprado por eBay en 2002) permite a personas y negocios con cuentas de correo electrónico hacer y recibir pagos hasta un límite especificado. Paypal transfirió aproximadamente $45 millones en pagos entre individuos y negocios en el 2007. Paypal ahora está disponible en 190 países y tiene cerca de 1958 millones de cuentahabientes, de los cuales aproximadamente 40 millones se consideran cuentas activas. Paypal se basa en la infraestructura financiera existente de los países en los que opera. Para establecer una cuenta de Paypal debe especificar una cuenta de crédito, de débito o de cheques en la que desee que se hagan los cargos o los pagos cuando realice transacciones en línea. Al hace un pago mediante Paypal, usted envía el pago por correo electrónico a la cuenta de Paypal del comerciante. Paypal transfiere el monto de su cuenta de crédito o de cheques a la cuenta bancaria del comerciante. La belleza de Paypal es que no se tiene que compartir información de crédito personal entre los usuarios, y el servicio puede ser utilizado por personas para pagarse unas a otras, incluso en pequeñas cantidades. Ente las desventajas de Paypal se encuentra: su alto costo, y la falta de protección para el consumidor cuando ocurre un fraude o se desconoce un cargo.

También hay varias categorías de valor almacenado en línea además de Paypal. Algunas como Valista, son plataformas mercantiles. Otras como QPass, están orientadas principalmente al mercado de micro pagos para los portadores inalámbricos y los editores que venden artículos individuales.

Las tarjetas inteligentes son otro tipo de sistema de valor almacenado que se basa en tarjetas de plástico del tamaño de una tarjeta de crédito, con chips incrustados que almacena información personal, la cual se puede utilizar para soportar los pagos.

El comercio electrónico móviles inalámbricos. No se utilizan desde las Pcs domésticas para comprar artículos, sino por lo general para pagar artículos de bajo costo pasando la tarjeta ante un lector, o deslizándola a través de éste. Mientras que las tarjetas de crédito almacenan un solo número de cuenta de cargo en la tira

magnética de la parte posterior, las tarjetas inteligentes pueden contener 100 veces más datos, incluyendo varios números de tarjetas de crédito e información relacionada con seguros de salud, transporte, identificación personal, cuentas de banco y programas de lealtad, como las cuentas de viajero frecuente. Esta capacidad las convierte en una alternativa atractiva en vez de portar una docena o más tarjetas de crédito y de identificación en una cartera física. Las tarjetas inteligentes también pueden requerir una contraseña, a diferencia de las tarjetas de crédito, lo cual agrega otro nivel de seguridad.

En realidad hay dos tipos de tarjetas inteligentes (de contacto y sin contacto), dependiendo de la tecnología incrustada. Para poder leer las tarjetas de contacto, deben colocarse físicamente dentro de un lector de tarjetas, mientras que las tarjetas sin contacto tienen una antena integrada que permite la transmisión de datos sin contacto directo mediante el uso de tecnología REFID. La identificación por radiofrecuencia (RFID) es un método de identificación automático que utiliza señales de radio de corto alcance para identificar objetos y usuarios. Una tarjeta inteligente de valor almacenado, como una tarjeta de regalo de una tienda de ventas al detalle comprada en determinado valor en dólares, es un ejemplo de una tarjeta de contacto ya que debe pasarse a través de un lector de tarjetas inteligentes para poder procesar el pago. Un sistema de pago de cuotas de carreteras como EZPass es un ejemplo de una tarjeta inteligente sin contacto, ya que el dispositivo EZPass en la tarjeta es leído por un sensor remoto, y la tarifa correspondiente se deduce automáticamente de la tarjeta al final del viaje.

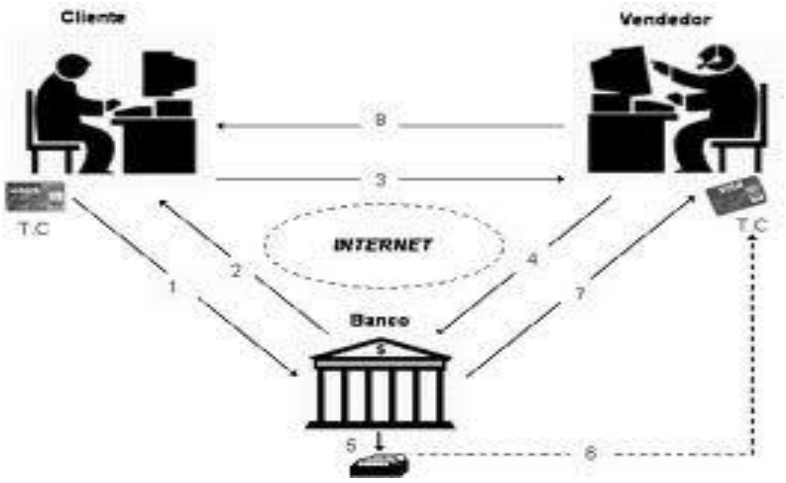

Figura 2. Esquema General Tarjeta Inteligente Mondex

Fuente: (Información Tecnológica, 2005)

Las tarjetas inteligentes como instrumentos de pago son más comunes en Europa y Asia. La tarjeta Mondex es una de las tarjetas originales, inventadas en 1990 por el banco NatWest Bank en Inglaterra. La tarjeta permite a los usuarios descargar efectivo de una cuenta de banco a la tarjeta, a través de un teléfono compatible con Mondex o de un lector de tarjetas conectado a una PC, y pueden gastar cantidades grandes o pequeñas. Puede llevar cinco monedas distintas al mismo tiempo y es aceptada por los comerciantes que tienen lectores instalados, ver figura 2.

Según Espineira y asociados (2005), la tarjeta Octopus es una tarjeta inteligente de valor almacenado sin contacto recargable, que se utiliza en Hong Kong. Hizo su debut en 1997 como un sistema de recolección de tarifas para el sistema de transporte masivo de Hong Kong. Hoy en día se ha convertido en la tarjeta inteligente de valor almacenado más exitosa en el mundo. Se puede utilizar para pagar no sólo el transporte público, sino también para realizar pagos en tiendas de de conveniencia y restaurantes de comida rápida, además del estacionamiento, y en las aplicaciones de punto de venta como las gasolineras y máquinas expendedoras, ver figura 3. Para enero de 2007 había más de 14 millones de tarjetas Octopus en circulación, utilizadas para llevar a cabo más de 12 millones de transacciones al día. La tarjeta se puede recargar en línea, en el mostrador de una

tienda o a través de máquinas de propósito especial de “valor agregado”. Hasta ahora, las tarjetas inteligentes han desempeñado un rol limitado en el soporte de transacciones electrónicas al instante, donde el usuario es móvil (como un pasajero en un tren subterráneo) y desea realizar pagos pequeños. Sin embargo, en el futuro la tecnología de las tarjetas inteligentes se integrará con los teléfonos celulares, y el pago inalámbrico para apoyar el comercio electrónico móvil tendrá un uso más amplio.

Figura 3. Tarjeta Octopus.
Fuente: (Información Tecnológica, 2005)

Sistema de Pago de Saldo Acumulado Digital

Los sistemas de pago de saldo acumulado permiten a los usuarios realizar micro pagos y compras Web, ya que acumulan un saldo de débito que se cobra a fin de mes. Al igual que una factura por servicios públicos o por servicio telefónico, se espera que los consumidores paguen el saldo completo al final del mes, usando una cuenta de cheques o tarjetas de crédito. Los sistemas de pago de saldo acumulado son ideales para comprar propiedad intelectual en Web, cómo pistas de música individuales, capítulos de libros o artículos de un periódico, o bien tonos para celular

o juegos. Los saldos se acumulan y los clientes reciben una factura mensual con su factura regular por su servicio telefónico.
Clickshare toma un enfoque distinto. Los consumidores tienen una cuenta en un sitio Web de su elección, y pueden utilizar esa cuenta para comprar contenido digital de otros sitios Web sin tener que introducir la información de su tarjeta de crédito u otro tipo de datos personales. Clickshare ha tenido su mayor aceptación en la industria de los periódicos y editoriales en línea, y a firmado trato con periódicos tan diversos como Chicago, Sun-Times, y con editoriales como Crain Communications. También posee servicios de cobro por suscripción, autenticación y transacciones para varios sitios Web de suscripción de los principales periódicos dirigidos a fanáticos de la NFL.

Sistemas de Pago con Cheques Digitales

En diciembre de 2004, la Reserva Federal estadounidense anunció que por primera vez en la historia el número de transacciones de pagos electrónicos (crédito, débito y otras) excedió al número de cheques en papel. Sin embargo, el vulnerable cheque no está preparado para retirarse todavía. En 2006 se escribieron más de 35 mil millones de cheques en EUA. Los sistemas de pago con cheques digitales buscan extender la funcionalidad de las cuentas de cheques existentes, para usarlas como herramientas de pago de compras en línea.

El sistema PayByCheck se basa en la cuenta de cheques existente del consumidor. Cuando un consumidor desea pagar con cheque en un sitio mercantil ofrece este servicio, aparece un formulario de autorización en línea que imita la apariencia de un cheque de papel. Se pide al usuario que llene la información de su cuenta en cheques, incluyendo un número de cheque valido, código de identificación bancaria y número de cuenta bancaria. Para autorizar el pago, un usuario debe escribir su nombre completo y, en ciertos casos si lo requiere el comerciante, los últimos cuatro número de su seguro social. La información del pago se verifica con las diversas bases de datos de PayByCheck que contiene información sobre escritores de

cheques falsos, información en tiempo real del banco del cliente sobre el estado de cuenta bancaria actual, base de datos de fraude y un sistema de verificación de direcciones para verificar el nombre y la dirección del cliente. También se puede usar la bioidentificación en forma de un escáner de huellas digitales conectado a una PC. Después, PayByCheck produce un cheque o débito electrónico para el monto de la compra, según lo indicado en el cheque y lo entrega al comerciante. El cheque es depositado en la cuenta del comerciante y se envía al banco del consumidor para su pago, de igual forma que un cheque escrito de una chequera. Las chequeras digitales no han tenido tanto éxito debido a las dificultades de verificar al cliente en línea.

Sistemas de Pagos Inalámbricos

Según Espiñeira y asociados (2005), hay aproximadamente 3 mil millones de teléfonos celulares en uso alrededor del mundo, y en China el número de teléfonos celulares sobrepasó los 300 millones en julio de 2007, un poco más que toda la población de EUA. La existencia de teléfonos celulares en EUA se estima ahora en 250 millones. Estos números hacen ver pequeña a la población mundial de computadoras personales de alrededor de 1 mil millones (TIA, 2007; eMarketer, Inc., 2007). En Japón, más de 95% de los hogares tiene teléfonos celulares.

El uso de los auriculares móviles como dispositivos de pago está muy bien establecido ya en Europa, Japón y Corea del Sur. Japón es sin duda el más avanzado en términos de proveer servicios que no son de voz para los consumidores; es decir, un verdadero comercio móvil. Los teléfonos celulares japoneses pueden actuar como lectores de código de barras, localizadores GPS, radios FM, grabadoras de voz y sintonizadores análogos de TV, también se pueden comprar cosas como boletos de tren, periódicos, comidas en restaurantes, abarrotes, libros y una variedad de artículos y servicios comunes de ventas al detalle. En Japón se utilizan 3 tipos de sistemas de pagos móviles, y éstos ofrecen un vistazo al futuro de los pagos móviles en EUA. Los teléfonos celulares japoneses

soportan dinero electrónico (sistemas de valor almacenado que se cargan mediante tarjetas de crédito o cuentas bancarias), tarjetas de débito móviles. Los teléfonos celulares japonés actúan como carteras móviles, ya que contienen una variedad de mecanismos de pago. Los consumidores pueden pagar a los comerciantes con sólo pasar su cédula frente a un dispositivo de pago mercantil que puede aceptar pagos. ¿Cómo se comunican los teléfonos celulares con los comerciantes, por ejemplo al comprar un periódico en una estación de tren o una comida en un restaurante? En 2004, NTT DoCoMo, la compañía telefónica más grande de Japón, introdujo los teléfonos celulares RFID inalámbricos y un sistema de pagos relacionado (FeliCa). Actualmente, en Japón se utilizan 10 millones de teléfonos carteras.

En Estados Unidos de América el teléfono celular todavía no ha evolucionado en un sistema de comercio y pago móvil con toda su capacidad. La gran mayoría de los ingresos de teléfonos celulares en EUA (estimados en $134 mil millones en 2007) provienen de los servicios de voz y no de los servicios de datos, información o juegos (de tan sólo $10 mil millones). En EUA, los usuarios de teléfonos celulares descargan en su mayor parte tonos de música y pagan a la compañía telefónica en su factura del mes siguiente. En Estados Unidos de América el teléfono celular no está conectado a la amplia red de instituciones financieras, sino que reside detrás del jardín amurallado de la variedad de artículos y servicios reales, y ahí los teléfonos se integran en un extenso arreglo de instituciones financieras (eMarketer, Inc., 2007). La historia de la sección Una perspectiva sobre negocios llamada El futuro del pago móvil: WavePayMe, TextPayme ofrece un vistazo al futuro del comercio móvil en Estados Unidos.

DERECHOS DE PRIVACIDAD DE INFORMACIÓN

La privacidad es el deseo moral de las personas a quedarse solas, libres de la vigilancia o la interferencia de otras personas u organizaciones, incluyendo al estado. La privacidad es una viga sobre la cual se apoya la libertad: sin la privacidad

requerida para pensar, escribir, planear y asociar de manera independiente y sin temor, la libertad social y política se debilita y tal vez se destruya. La privacidad de información es un subconjunto de la privacidad. El derecho a la privacidad de la información incluye tanto la afirmación de que los gobiernos o empresas no deben recabar determinada información de ninguna forma, como el reclamo de las personas a controlar el uso de cualquier información que se recolecte sobre ellas. El control individual sobre la información personal está en el núcleo del concepto de privacidad.

El proceso legal establecido también desempeña un rol importante para definir la privacidad. La doctrina de las Prácticas Justa de Información proporciona la mejor declaración del proceso legal establecido en el mantenimiento de registros. Esta doctrina se desarrolló a principios de la década de 1970 y se extendió al debate sobre la privacidad en línea a finales de la década de 1990.

Hay dos tipos de amenazas a la privacidad individual que plantea Internet. Una amenaza se origina en el sector privado y se refiere a cuanta información personal se recolectan en los sitios WEB privados, y como se utilizará. Una segunda amenaza se origina en el sector público y se refiere a la cantidad de información personal que recolectan las autoridades locales, estatales, federales y como la utilizan.

Los reclamos de privacidad brotaron rápidamente en Estados Unidos de América al final del siglo XIX, a medida que la tecnología de la fotografía y el periodismo sensacionalista permitió la invasión de las vidas (que hasta ese momento eran privadas) de los industriales ricos. Sin embargo en la mayor parte del siglo XX el pensamiento sobre la privacidad y la legislación se enfocaron en restringir al gobierno la captación y uso de información personal. Con la explosión de la recolección de información personal privada por parte de las empresas privadas por parte de las empresas de marketing basado en WEB desde 1995, las cuestiones

sobre la privacidad están cada vez más orientadas a restringir las actividades de las empresas privadas en cuanto a la recolección y uso de la información en Web.
En general Internet, Internet y Web proporcionan un entorno ideal para que los negocios y el gobierno invadan la privacidad personal de millones de usuarios en una escala sin precedentes en la historia. Tal vez ninguna otra cuestión reciente ha generado una preocupación social y política tan extendida como la protección de la privacidad de entre 175 y 200 millones de usuarios Web, tan solo en EUA.

GOBIERNO CORPORATIVO, GESTIÓN RIESGO Y CUMPLIMIENTO DE LEY (GR&C)

Herrera (2008), las organizaciones desafían constantemente los retos que significa mantener una buena reputación en el mercado, motivado a la presión que día a día ejercen los accionistas e inversionistas con el objeto de asegurarse que la empresa sea rentable, se encuentre adecuadamente controlada y en cumplimiento de las regulaciones de ley. Dicha presión se ha incrementado notablemente en los últimos años, debido a los múltiples escándalos financieros ocurridos en grandes industrias que a la vista pública, lucían sólidas. Es por ello que cada vez más los presidentes y miembros de las juntas directivas de las compañías, necesitan contar con un gobierno corporativo adecuadamente implementado, a fin de proteger su reputación y los intereses de los accionistas.

Las compañías que desarrollan sólidos programas de Gobierno Corporativo, Gestión de Riesgo y Cumplimiento de Ley, atraen a los inversionistas, ganan la confianza pública y construyen organizaciones financiera y estratégicamente viables que permiten realzar, por largos períodos, el valor del accionista.

La importancia de los programas de gobierno Corporativo, Gestión de Riesgo y Cumplimiento de Ley (GR&C- siglas de inglés de Governance, Risk and Compliance), se debe a varios factores, entre los que se encuentran:

- Surgimiento de nuevas legislaciones corporativas.
- Desarrollo de nuevas y complejas regulaciones que deben ser cumplidas por las organizaciones (Ej.: Ley Sarbanes-Oxley, HIPAA, Basilea, entre otros).
- Globalización y expansión de las operaciones de las compañías en nuevos países.

En consecuencia, las organizaciones que no lleven a cabo programas para el establecimiento de un GR&C en el mediano plazo, estarán corriendo el riesgo de:

- Perjudicar la reputación de la compañía y la habilidad de retener tanto a clientes como empleados.
- Pérdida de ganancias y nuevas oportunidades de negocio.
- Penalidades por el incumplimiento de regulaciones de ley impuestas por entes legisladores locales e internacionales.
- Posibles procesos de litigio.

¿QUÉ ES EL GOBIERNO CORPORATIVO (GOVERNANCE)?

Gobierno Corporativo (Governance) es el proceso y estructura utilizada para dirigir y administrar el negocio y las relaciones corporativas, con el objetivo de realzar el valor para el accionista y los grupos de interés. Dichos procesos y estructura definen las divisiones de poder y establecen mecanismos para conseguir la responsabilidad entre los accionistas, la junta directiva y la gerencia del negocio.

Las características fundamentales para que un Gobierno Corporativo tenga efecto en una organización, son las siguientes:

- Transparencia: informar de manera clara y completa a los accionistas de las actividades financieras y administrativas de la compañía, instaurando una cultura de integridad e imparcialidad.

- Supervisión: establecer controles internos y externos lo suficientemente sólidos, que permitan instruir un comité dedicado al cumplimiento de ley, integridad y gestión del riesgo.
- Responsabilidad: contar con estructuras de negocio y gerenciales abiertas, teniendo en cuenta el impacto que la gerencia tienen en los empleados, clientes y proveedores, así como la creación de valor en el negocio.
- Adaptabilidad: contar con estructuras de negocios que puedan adaptarse y evolucionar ante los cambios sociales, de mercado y de competencia con otras empresas del sector o industria, desarrollando una fuerza de trabajo comprometida a "auto-monitorearse".

Una junta directiva dedicada, comprometida y dinámica es el corazón de un buen Gobierno Corporativo.

¿QUÉ ES GESTIÓN INTEGRAL DE RIESGO, GIR (ENTREPRISE RISK MANAGEMENT – ERM)?

La GIR según el autor anteriormente citado se define como:

"Proceso influenciado por la junta directiva, directores, gerencia y el personal, aplicado para establecer estrategias y que se ejecuta sobre toda la empresa o corporación, diseñado para identificar eventos potenciales que pudieran afectar al negocio y que ayuda a gerenciar los riesgos dentro del marco organizacional, todo esto para proveer un nivel razonable de seguridad en el camino de cumplir sus objetivos de negocio".

Los beneficios de la Gestión Integral de Riesgo en las corporaciones se basan en que no existe ningún negocio que se encuentre exento de riesgos o se desenvuelva en un ambiente, interno o externo libre de éstos. En consecuencia, la GIR le permite

a la gerencia operar más eficientemente en ambientes propensos a riesgos, con lo cual se garantiza la capacidad del negocio para:

Alinear el apetito de riesgo y la estrategia. El apetito de riesgo es el grado de riesgo que, en general, una compañía está dispuesta a aceptar en persecución de sus metas y objetivos. La gerencia, en primer lugar, considera el apetito de riesgo en la compañía para evaluar alternativas estratégicas. En segundo lugar, establece objetivos alineados con la estrategia seleccionada y desarrolla mecanismos que permitan gerenciar los riesgos relacionados.

Interconectar el crecimiento, el riesgo y la rentabilidad. Las compañías aceptan el riesgo como parte de la creación de valor y preservación, esperando una rentabilidad y crecimiento proporcional al riesgo asumido. La GIR provee destrezas para identificar y medir cualitativa y cuantitativamente el impacto de los riesgos, así como para establecer niveles aceptables de riesgos relativos a los objetivos de crecimiento y rentabilidad establecidos.

Mejorar las decisiones en respuesta a los riesgos. La GIR provee lineamientos rigurosos para identificar y seleccionar respuestas a los riesgos entre varias alternativas, así como para eliminar, reducir, compartir y aceptar los riesgos.

Minimizar sorpresas operacionales y pérdidas. Las compañías pueden mejorar su capacidad para identificar potenciales eventos de riesgo, medir y establecer respuestas a los mismos, así como reducir la ocurrencia de sorpresas en la operación del negocio y relacionadas a costos y pérdidas.

Identificar y gerenciar riesgos inter-organizacionales. Las compañías afrontan un conjunto de riesgos que afectan a distintas partes de la organización. La gerencia necesita, no únicamente administrar riesgo de manera individual, sino también entender el impacto que los mismos pudiesen ocasionar al interrelacionarse.

Proveer respuestas integradas a múltiples riesgos. Los procesos de negocio conllevan una gran cantidad de riesgos inherentes y la GIR permite integrar soluciones para administrarlos.

Aprovechar las oportunidades. La gerencia debe considerar y analizar los eventos potenciales que puedan afectar los objetivos estratégicos, por no tan solo enfocado en los riesgos, sino obteniendo el conocimiento de cómo los eventos pudieran representar oportunidades.

Racionalización del capital. En la medida que la GIR maneje una sólida información de los riesgos de la empresa o corporación, podrá obtener evaluaciones más efectivas acerca del capital necesario y de las correspondientes provisiones.

¿QUÉ ES EL CUMPLIMIENTO DE LEY (COMPLIANCE)?

Es el modelo organizacional, procesos y sistemas de una empresa o corporación, utilizados para asegurar que sus estructuras, reputación y condición financiera estén en concordancia con las leyes, regulaciones de ley, estándares internos y políticas, así como las expectativas de los accionistas, clientes, proveedores, empleados y sociedad en general.

El cumplimiento de Ley es una función, la cual es llevada a cabo por un equipo independiente en la organización y que sirve de apoyo a las funciones del gobierno Corporativo y la GIR. Más allá de una función de auditoría interna, la función del Cumplimiento de Ley necesita estar cerca del día a día de las unidades de negocio, a fin de identificar riesgos potenciales de cumplimiento a nivel operacional y ayudar a resolverlos.

Las mejores prácticas proveen un marco de siete (7) criterios para llevar a cabo la administración de los riesgos de cumplimiento de la compañía, los cuales pueden observarse en la tabla 2.

MODELO INTEGRADO DE GOBIERNO CORPORATIVO, GIR Y CUMPLIMIENTO DE LEY (GR&C)

Existen diversos enfoques que guían y ayudan en la implementación de esquemas de GR&C en las compañías. El modelo integrado que se muestra en la Figura Nº4, se focaliza en crear, en todos los niveles de la organización, un compromiso con la Gestión de Riesgo y el Cumplimiento de Ley. En este sentido, el modelo establece tres (3) elementos básicos, a saber:

Por medio de la junta directiva y la gerencia. La ética en los negocios establece la dirección de cómo una compañía cultiva la cultura de “hacer lo correcto” e integra los valores principales, tales como responsabilidad y confianza, en toda la organización. Tanto la junta directiva como la gerencia, necesitan contar con una visión sólida y unificada del propósito de un programa de GR&C. La gerencia es responsable de planificar e implementar un programa efectivo, mientras que la junta directiva supervisa las actividades realizadas por ésta, a fin de asegurar que la implementación ocurra y que las responsabilidades corporativas sean conocidas.

Mediante un código de conducta canalizador de valores. Los valores sirven de guía en los procesos de toma de decisión y determinan cómo la compañía se conducirá en tiempos de incertidumbre. La ética y valores de la compañía en relación con GR%C necesita “vivir” y estar inmersa en el código de ética o conducta, el cual es importante comunicar a todos los empleados y terceras partes asociadas. El código de ética o conducta no sólo debe expresar los valores gerenciales, sino también identificar y reflejar los valores de los accionistas.

Mediante la integración efectiva en los procesos de negocio. La integración con los procesos de negocio incluye desarrollar políticas y procedimientos, comunicarlas y adiestrar a los empleados en el manejo de las mismas y del código de conducta; monitorear el progreso, reportar a la gerencia y a la junta directiva, así como a los accionistas. La integración asegura que el programa de GR&C se convierta en operacional y efectivo.

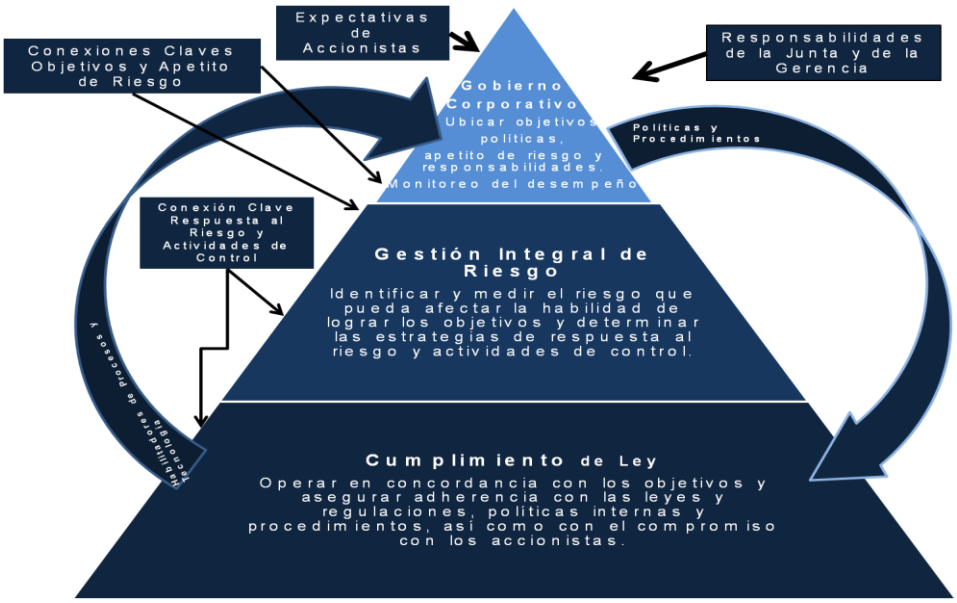

Figura 4. Modelo integrado de Gobierno Corporativo, Gestión de Riesgo y Cumplimiento de Ley (GR&C).

Fuente: (Espiñeira, Sheldon y Asociados 2006, p. 105).

Adicionalmente, el modelo antes expuesto se basa en ocho (8) elementos clave para componer una efectiva gestión de GR&C, los cuales son:

- Código de ética y de conducta corporativo.
- Políticas y procedimientos.
- Adiestramiento en Cumplimiento de Ley y ética.
- Demostrar el comportamiento esperado (“ser ejemplo”).
- Continuidad del proceso de mejoramiento.
- Reporte en tiempo real
- Monitoreo y medición del desempeño de la gestión de GR&C.

- Información consistente, completa, a tiempo y precisa.

Cuando se diseña una función de GR&C, la organización debe considerar tanto los roles funcionales y las responsabilidades, como las nuevas tecnologías, estándares en políticas y procedimientos, que subsecuentemente serán incorporados al programa. En este sentido, en la tabla 3, se detallan los roles y responsabilidades bajo un modelo integrado de GR&C.

Tabla 3. Criterios para un programa efectivo de Cumplimiento de Ley.

Criterio	Indicadores de alto nivel / Preguntas de Autoevaluación
Procedimientos y estándares de cumplimiento de ley.	¿Existen políticas y procedimientos de Cumplimiento de Ley amplios y consistentes a lo largo de toda la organización? ¿El código de conducta es una declaración resumida, proactiva y completa de la posición de la organización sobre la ética y el Cumplimiento de Ley?
Oficial de Cumplimiento	¿Existen responsabilidades específicas para el Cumplimiento de Ley asignadas a la junta directiva y a la gerencia? ¿La línea de reporte y estructura establecida para el Oficial de Cumplimiento de Ley asegura la independencia y efectividad de la gestión y sus integrantes?
Precaución en la delegación de autoridad	¿Están adecuadamente establecidas las delegaciones financieras y las líneas de decisión? ¿se realizan auditorías sobre la gestión de los agentes, consultores y otros socios de negocio? ¿la organización lleva a cabo un monitoreo detallado de las acciones disciplinarias?
Comunicación efectiva	¿La compañía lleva a cabo adiestramientos periódicos en cuanto a Cumplimiento de Ley y conciencia corporativa para todos sus empleados? ¿El adiestramiento se enfoca en aquellas áreas de la organización donde las responsabilidades son sensibles al Cumplimiento de Ley?

Monitoreo, auditoría y reporte	¿Existe una clara definición de la línea de reporte organizacional para que los empleados puedan estar en contacto y buscar ayuda o reportar eventos inusuales o denuncias de violación al código de ética o conducta? ¿La compañía posee un mecanismo para garantizar la confidencialidad y anonimato de aquellos empleados que reporten preocupaciones o temas relacionados con aspectos éticos? (Por ejemplo, líneas telefónicas directas o una cuenta de correo confidencial)
Disciplina constante	¿La compañía demuestra motivación e interés en reforzar el Cumplimiento de Ley, tomando acciones disciplinarias contra aquellos empleados que incumplan con las políticas de la organización, sin importar su posición organizativa? ¿La conducta ética es incluida como parte del desarrollo individual en las evaluaciones de desempeño y como pronosticador para el avance del empleado en la organización?
Modificación de procesos	¿La compañía mantiene registro de material relacionado con el cumplimiento de Ley que pueda ser necesitado en futuros eventos o investigaciones? ¿La compañía monitorea de manera proactiva asuntos potenciales y áreas de alto riesgo, a fin de responder a problemas y determinar cuáles son las acciones necesarias que deberían tomarse?

Fuente: (Herrera, 2008).

Tabla 4. Roles y responsabilidades bajo un modelo GR&C.

Nivel Empresarial	Soporte Funcional del Programa Empresarial
Proveer coordinación centralizada y supervisar con apoyo del comité de GR&C. Definir y comunicar la visión, objetivos y políticas empresariales. Desarrollar planes anuales de riesgo y Cumplimiento de Ley. Asegurar qué las políticas consistentes son adoptadas a través de todas las funciones de la compañía. Establecer un plan de adiestramiento que abarque toda la organización. Proveer una función que se encargue de responder preguntas y canalice situaciones relativas a GR&C. Proveer de herramientas y tecnología para la implementación y evaluación del modelo de GR&C. Definir identificadores clave para ser utilizados como base en programas de evaluación y mejoramiento continuo. Monitorear el desempeño de los programas tanto empresariales como funcionales. Crear una estructura y protocolo para coordinar investigaciones y acciones disciplinarias. Coordinar las mejores prácticas y lecciones aprendidas. Identificar situaciones emergentes relativas a GR&C. Reportar a la junta directiva y a la gerencia el desarrollo del programa, y desarrollar indicadores de gestión. Identificar oportunidades que permitan mejorar el proceso.	Implementar un marco empresarial de manera que sea consistente con el modelo de GR&C y soporte las necesidades funcionales. Controlar las herramientas empresariales y tecnologías que apoyen el programa. Proveer un plan de adiestramiento y comunicación, enmarcado dentro del marco organizacional. Monitorear y medir el desempeño del programa, utilizando indicadores de gestión establecidos. Identificar posibles riesgos y desarrollar controles que permitan mitigarlos. Reportar la efectividad del programa, incluyendo incidentes gerenciales. Identificar las mejores prácticas y lecciones aprendidas, para el mejoramiento continuo.

Fuente: (Herrera, 2008)

COMPONENTES DE LA GIR

Según Espiñeira y Asociados (2006), la GIR está constituida por ocho componentes interrelacionados. Estos componentes se derivan de cómo la gerencia maneja o administra y de cómo la interrelación e integración de estos componentes están implantados en los procesos del negocio. Los ocho (8) componentes de la GIR son:

Ambiente de Control: es la base para los demás componentes y su principal objetivo es dar disciplina y estructura. Entre los factores influenciados por el ambiente de control están la estrategia y los objetivos están establecidos o implantados, las actividades del negocio son estructuradas y los riesgos identificados, los riesgos son evaluados, la entidad o empresa o corporación afronta los riesgos, el diseño y funcionamiento de las actividades de control, el control de los sistemas de información y comunicación, y se estructuran y ejecutan las actividades de monitoreo. El ambiente de control contiene varios elementos entre ellos están los valores éticos de la entidad o empresa, la competencia y el desarrollo del personal, el estilo de operación de la gerencia el cual incluye la asignación de autoridades y responsabilidades.

La GIR debe garantizar la vigencia y aplicación del código de ética y conducta, así como promover la honestidad y la conducta ética, incluyendo el manejo ético, real o aparente, de los conflictos de intereses entre las relaciones personales o profesionales, además es importante que todo el personal de la empresa acepte y cumpla las normas en dicho expuestas en dicho manual.

Establecimiento de Objetivos, corresponde a la fijación de los objetivos o metas que la empresa desea alcanzar en un período determinado, los cuales deben estar presentes, antes que la gerencia pueda identificar los eventos que potencialmente afectan sus metas. Los objetivos pueden ser clasificados en cuatro categorías:

Estratégicos: tienen relación con metas de alto nivel, dando así apoyo a la misión y visión del negocio. Operacionales: están relacionados con la efectividad y eficiencia de las operaciones de la empresa, en ocasiones varían dependiendo de las decisiones tomadas por la gerencia ya sea en cuanto a estructura y/o rendimiento.

Reporte: es la forma de informar los resultados financieros y operativos de manera efectiva. Cumplimiento: Cumplimiento de las leyes y regulaciones a través del comportamiento en las actividades de la gerencia.

El fin de los objetivos es que de manera estructurada puedan evaluar y dar seguimiento a los objetivos a través de la GIR.

Identificación de Eventos, este componente consiste en la identificación de los eventos potenciales que afectan o impactan a la entidad o empresa o corporación, incluyendo los factores internos y externos. Esto incluye cómo los eventos pudieran impactar o afectar las metas y objetivos estratégicos, están consiente que se maneja cierto grado de incertidumbre, en ese sentido hay factores externos como por ejemplo la economía, la política, el ámbito social, tecnológico que pueden en cierto momento afectar a la empresa, y factores internos tales como: personal, la infraestructura, procesos, tecnología que los impacta. Existen diversas técnicas y herramientas para identificar los eventos, entre ellos las experiencias previas y predicciones de acuerdo a sucesos que ocurrieron en su oportunidad y pueden volver a ocurrir. Los eventos mayormente tienen impactos negativos por eso la importancia de prevenir y estar pendiente de las situaciones presentadas, hay eventos positivos o negativos y positivos. Se dice que tienen un impacto negativo cuando ocasionan riesgos y por lo tanto requieren de una revisión y evaluación y determinar cuál es la solución. El riesgo en general lo definen como la posibilidad que un evento pueda ocurrir y causar impacto en los objetivos previsto en el negocio.

Evaluación de Riesgos, consiste en el análisis de los riesgos a los fines de construir las bases y decisiones que llegarán a la determinación de qué y cómo hacer para manejar los riesgos.

Es de resaltar que los riesgos están asociados con los objetivos que puedan ser afectados. Para realizar la medición del riesgo utilizan una metodología la cual contiene técnicas cualitativas y cuantitativas, la gerencia utiliza técnicas cualitativas de evaluación, ya que los riesgos no son fáciles de cuantificar o cuando se hace necesario l acumulación y recolección de datos complejos. Las técnicas de cuantificación, típicamente brindan mayor precisión y son mayormente utilizadas en actividades más complejas y sofisticadas con el de completar las técnicas de cualificación.

Usualmente, la gerencia utiliza indicadores de medición de rendimiento para determinar los avances o niveles de cumplimiento de las metas trazadas. Es recomendable utilizar la misma unidad de medida cuando se considera el impacto potencial del riesgo en cumplimiento de un objetivo específico, la gerencia por tanto debe evaluar cómo se correlacionan los eventos, donde la secuencia de estos eventos y su interacción crean diferentes probabilidades e impactos, mientras que el impacto de un simple evento pudiera ser bajo, una secuencia de eventos pudiera tener un impacto significativo.

Respuesta al Riesgo, el cual incluye la identificación de las opciones de respuesta u opciones para enfrentar los riesgos, tomando en cuenta la tolerancia al riesgo, el apetito de riesgo y los costos y beneficios para la organización. La respuesta al riesgo caen dentro de las categorías de riesgo, las cuales permiten: evitarlo, reducirlo, compartirlo o aceptarlo. La respuesta de evitarlo significa salirse de la actividad que elevan o incrementan el riesgo. Reducirlo permite minimizar la certidumbre o impacto. Compartirlo reduce el impacto ya que comparten el riesgo.

Aceptarlo significa el no tomar acción alguna que pueda ser que modifique la certidumbre.

Actividades de Control, las cuales se refieren a las políticas y los procedimientos implantados y ejecutados por la entidad o empresa o corporación que están diseñados para responder efectivamente al riesgo.

Información y Comunicación, las cuales son las canales y sistemas para comunicarse con el personal de la entidad o empresa o corporación. En este componente se especifican los canales de comunicación que deben ser establecidos para lograr que fluya la información en diferentes situaciones, en particular en casos excepcionales, a lo largo de la entidad o empresa o corporación.

Monitoreo, el cual se debe ejecutar sobre los procesos de la GIR y que requieren ser modificados de acuerdo a las necesidades. Y se lleva a cabo a través de un proceso de evaluación de los componentes, su funcionamiento y calidad de su operación. El monitoreo puede hacerse en dos formas o vías, por medio de las actividades del día a día o mediante evaluaciones separadas.

Esta nueva estructura de componentes de la GIR, obliga a repensar la naturaleza del riesgo, su tratamiento y gerencia en las entidades o empresas o corporaciones.

DESCRIPCIÓN GENERAL DEL RIESGO OPERACIONAL.

Según Fontnouvelle, DeJesus, Jordan y Rosengren (2003), la aparición de grandes bancos internacionales activos diversificados, ha creado la necesidad de gestión de riesgos sofisticados. Las grandes instituciones dependen cada vez más de modelos estadísticos para evaluar el riesgo y asignar capital a través de la organización. Estos modelos son a menudo los principales insumos en los modelos RAR (Risk Asset Ratio), Santiago (1996), las decisiones de inversión, y la

determinación de las indemnizaciones y bonificaciones. Por lo tanto, los gerentes de línea tienen un fuerte incentivo para verificar la exactitud del riesgo y el capital atribuido a su área.

Como la gestión de riesgos se vuelve más sofisticada, los supervisores bancarios están alentando a los bancos para desarrollar sus modelos de riesgo, tanto por rating directamente la gestión de riesgos a través de la supervisión de procesos y mediante la incorporación de los modelos en el proceso de reglamentación. El riesgo de mercado fue la primera área migrar las prácticas de gestión del riesgo directamente en el proceso de reglamentación, el Riesgo de Mercado 1996 Enmienda al Acuerdo de Basilea, utilizó el valor en los modelos de riesgo para determinar el capital de riesgo de mercado para bancos grandes y complejos. Estos valores en los modelos de riesgo son ampliamente utilizados por las instituciones financieras. Sin embargo, la investigación sobre modelos de riesgo de mercado ha tendido a centrarse en los procedimientos de ejecución Hendricks (1996) y Pritsker (1997), en parte debido a la naturaleza propietaria de los modelos de Berkowitz y O'Brien (2002) fueron capaces de obtener valor a las previsiones de riesgo empleados por comercial bancos, pero el valor concertado en los modelos de riesgo no eran especialmente medidas precisas de riesgo de la cartera.

Los reguladores están aumentando el énfasis dado a modelos de riesgo de crédito. La Basilea propuesta es mucho más sensible al riesgo, y requiere detalle significativo en el cálculo del crédito de los bancos. Las preocupaciones por una mayor sensibilidad al riesgo. También llamado la atención académica Catarineu-Rabell, Jackson y Tsomocos (2002), Jordan, Peek y Rosengren (2003), pero si bien esta propuesta se pretende capturar la mejor prácticas en los principales bancos comerciales, la investigación académica de nuevo se ha visto entorpecido por la naturaleza propietaria de los datos y los modelos. Como resultado, la mayoría de los estudios de riesgo de crédito han examinado instrumentos de mercado similares, que están en mejores aproximaciones imperfectas para el riesgo de crédito real de un banco la exposición Carey (1998).

Del mismo modo, mientras que el trabajo de análisis de las instituciones financieras en el área de riesgo operacional tiene avanzado significativamente en algunas instituciones financieras, la investigación académica ha ignorado en gran medida el tema debido a la falta de datos. No sólo era tal propiedad de los datos, pero además, no era coherente la definición de una pérdida operacional dentro de las instituciones financieras. Como resultado, bases de datos internas y externas eran difíciles de desarrollar. Sin embargo, el Grupo de Gestión de Riesgos (RMG) del Comité de Basilea y representantes de la industria desarrollaron una definición estandarizada del riesgo operacional.

Su definición: "El riesgo de pérdida resultante de inadecuados o fallidos procesos internos, personas y sistemas o por eventos externos". La RMG también ha proporcionado líneas de negocio estandarizado y tipos de pérdida como vías generales de clasificación de eventos operacionales. Las líneas de negocio son: Finanzas Corporativas; Negociación y Ventas, Pago y Liquidación; Servicios de la Agencia; Banca Comercial, Gestión de Activos, y al por menor de Bolsa.

Los tipos de pérdidas son:

Fraude interno: en la práctica los bancos también se enfrentan a dificultades similares y recurren a datos externos.

La definición estándar incluye el riesgo legal, pero excluye el riesgo estratégico y reputacional.

Fraude externo: las prácticas de empleo y Seguridad en el Trabajo, Clientes, Productos y Empresas prácticas, perjuicios a activos materiales, interrupción de los negocios y el fallo del sistema, y de Ejecución, la entrega y gestión de procesos.

La adopción de las normas de Basilea ayudo a mejorar la coherencia de la recopilación de datos tanto dentro como entre las organizaciones bancarias.
Esta coherencia permitirá a los bancos para comparar su experiencia de pérdida a través de líneas de negocio, y para los supervisores para comparar la pérdida experiencia a través de los bancos. Los proveedores de datos externos también están aplicando las mismas normas, permitirá a los bancos para comparar su experiencia de pérdida con la de sus pares, y para aplicar los resultados a partir de datos externos para modelar sus propias exposiciones de riesgo.

INVESTIGACIONES FINANCIERAS DE ORIENTACIÓN

Durante la última revisión del Grupo de Acción Financiera (GAFI)(2012), una mayor atención se le dio a la lucha contra el lavado de dinero operativo / lucha contra la financiación del terrorismo, cuyos objetivos era reforzar las normas de aplicación de la ley (recomendaciones 30 y 31) para mejorar las funciones, responsabilidades, competencias y herramientas de la ley la ejecución para llevar a cabo con eficacia el lavado de dinero (LD), la financiación del terrorismo (FT) y activos, rastreo de investigaciones, las normas revisadas reconocen ahora las investigaciones financieras como uno de los elementos centrales de las recomendaciones operativas y de aplicación de la ley del GAFI. La orientación sólo se diseñó para ayudar a los países a entender el papel de la policía, dirigiéndose específicamente al papel de investigaciones financieras. La intención de la guía es ayudar a los responsables políticos, así como profesionales, proporcionando ideas y conceptos que pueden incorporar a su trabajo diario y que pueden llevar investigaciones financieras más eficaces. Estas ideas pueden ir más allá del alcance de las normas, pero están destinados a proporcionar ejemplos de las formas en que los países llevan a cabo investigaciones financieras, como beneficio adicional, la guía también puede ser útil para el futuro de evaluaciones y podría ayudar a los países en la mejora de la eficacia del funcionamiento.

OBJETIVOS Y BENEFICIOS DE LA INVESTIGACIÓN FINANCIERA

Los países deben asegurar que las investigaciones financieras se convierten en algo primordial en una organización, los principales casos de financiamiento del terrorismo procede de generación y sus principales objetivos son:

La identificación de productos del delito, la localización de activos y el inicio de los activos, medidas de confiscación, mediante medidas de carácter temporal, como la congelación / incautación cuando sea apropiado.

Inicio de investigaciones de lavado de dinero cuando sea apropiado.

El descubrimiento de las estructuras financieras y económicas, transnacional, interrumpir redes y la recopilación de conocimientos sobre los patrones de criminalidad.

Una investigación financiera consiste en la recogida, cotejo y análisis de todos los disponibles con miras a prestar asistencia en la represión de la delincuencia y en la privación de los productos e instrumentos del delito, los delincuentes por lo general les gusta mantener un cierto grado de control sobre sus activos, y como resultado, por lo general hay un "rastro de papel" que conducirá de nuevo al delincuente, ese rastro de papel también se puede seguir para identificar delincuentes adicionales y posiblemente la localización de pruebas e instrumentos utilizados para cometer los delitos, la capacidad de los organismos encargados de hacer cumplir la ley para llevar a cabo las investigaciones financieras y tener acceso a la información financiera, es esencial para luchar eficazmente contra el lavado de dinero, delitos conexos y los delitos de financiamiento al terrorismo, las investigaciones a menudo establecen la existencia de crímenes y activos que han sido adquiridos con el producto de la actividad delictiva, permitiendo así que estos activos se conviertan en objeto de confiscación.

BASES LEGALES

Constitución de la República Bolivariana de Venezuela

La Constitución Nacional de la República Bolivariana de Venezuela publicada en Gaceta Oficial Extraordinaria Nº 37.401 de fecha 11 de marzo del año 2002, es el documento vigente que contiene la Ley fundamental del país, dentro de cuyo marco deben ceñirse todos los actos legales. En ella se generan las instituciones, derechos y deberes fundamentales.

Ver tabla 5 para observar las bases legales de la investigación.

Tabla 5. Bases Legales de la Investigación

Base Legal	Gaceta	Leyes	Observaciones
Completa	Constitución de la República Bolivariana de Venezuela (Publicada en Gaceta Oficial del jueves 30 de diciembre de 1999, Número 36.860)	Carta Magna	Debe ser revisada en la ejecución del proyecto de investigación de maestría
Completa	Ley General de Bancos y Otras Instituciones Financieras Gaceta Oficial Nº 39.491 del 19 de agosto de 2010	Ley de los bancos, entidades de ahorro y préstamo, demás instituciones financieras, y casas de cambio	Debe ser revisada en la ejecución del proyecto de investigación de maestría
Completa	Ley contra los Delitos Informáticos Gaceta Oficial N° 37313 de fecha 30 de Octubre de 2001	Protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías	Debe ser revisada en la ejecución del proyecto de investigación de maestría
Art 4 y art 5	Ley Orgánica contra la Delincuencia Organizada	El objeto es prevenir, investigar, perseguir, tipificar y sancionar los delitos relacionados con la delincuencia organizada	Debe ser revisada en la ejecución del proyecto de investigación de maestría

GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL (GAFI)

El Grupo de Acción Financiera Internacional sobre el blanqueo de capitales (GAFI) es un organismo intergubernamental cuyo propósito es el desarrollo y la promoción de políticas, en los niveles nacional e internacional, para combatir el lavado de dinero y el financiamiento del terrorismo. Fue establecido en 1989 por el G7, y en abril de 1990 dio a conocer sus Cuarenta Recomendaciones, que proveen un diseño de la acción necesaria para luchar contra el lavado de dinero. Las mismas fueron revisadas en 1996 y reformuladas sustancialmente en 2003 para reflejar los cambios en las tendencias del lavado de dinero y anticipar futuras amenazas.

En 2001, se emitieron las 8 Recomendaciones Especiales para combatir el Financiamiento del Terrorismo, que fueron complementadas en octubre de 2004 con la emisión de la 9º recomendación especial referida al movimiento transfronterizo de efectivo. La sede del organismo está en París, y su estructura incluye Grupos de Trabajo y Plenario. En los Grupos de Trabajo se encuentra el de Tipologías, Lavado de Dinero y Financiación del Terrorismo, entre otros. Las reuniones tanto de los grupos de trabajo como del plenario son tres veces al año. El GAFI emite recomendaciones, evaluaciones mutuas de países, “follow up” seguimientos, y sanciones; además de proveer capacitación para sus miembros.

COMITÉ DE BASILEA

El Comité de Basilea es la denominación usual con la que se conoce al Comité de Supervisión Bancaria de Basilea (BCBS, sigla de Basel Committee on Banking Supervisión en inglés), la organización mundial que reúne a las autoridades de supervisión bancaria, cuya función es fortalecer la solidez de los sistemas financieros.

Entre las normas de importancia que el Comité ha emitido, se encuentran las recomendaciones sobre blanqueo de capitales.

Basilea I: acuerdo publicado en 1988, en Basilea, Suiza, por el Comité de Basilea, compuesto por los gobernadores de los bancos centrales de Alemania, Bélgica, Canadá, España, EE. UU., Francia, Italia, Japón, Luxemburgo, Holanda, el Reino Unido, Suecia y Suiza. Su fin, fortalecer el sistema bancario, mejorando la comprensión de los principales problemas de supervisión y la calidad de supervisión. Marco pauta por la creación de las normativas internacionales sobre la adecuación del capital.

Basilea II: es el segundo de los Acuerdos de Basilea. Dichos acuerdos se basaron en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea. El propósito de Basilea II, publicado inicialmente en junio de 2004, es la creación de un estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

Basilea III: Surge tras la crisis financiera, se refieren a un conjunto de propuestas de reforma de la regulación bancaria, publicadas a partir del 16 de diciembre de 2010. Refuerza requisitos de capital bancario e introduce nuevos requisitos.

SUPERINTENDENCIA DE LAS INSTITUCIONES DEL SECTOR BANCARIO (SUDEBAN)

La Superintendencia de las Instituciones del Sector Bancario es el ente de regulación del sector bancario bajo la vigilancia y coordinación del Órgano Superior del Sistema Financiero Nacional. Es una institución autónoma con personalidad jurídica y patrimonio propio e independiente de los bienes de la República, y se

regirá por las disposiciones que establezcan la Ley General de Bancos y Otras Instituciones Financieras, gaceta oficial Nº 6.015 Extraordinario del 28 de diciembre de 2010.

Corresponde a esta Superintendencia autorizar, supervisar, inspeccionar, controlar y regular el ejercicio de la actividad que realizan las instituciones que conforman el sector bancario, así como, instruir la corrección de las fallas que se detecten en la ejecución de sus actividades y sancionar las conductas desviadas al marco legal vigente. Todo ello con el fin de garantizar y defender los derechos e intereses de los usuarios y usuarias del sector bancario nacional y del público en general.

El área medular de la Sudeban supervisa, regula y previene a través de 12 Gerencias de Inspección, las cuales tienen la responsabilidad de instrumentar dos tipos de controles fundamentales: el Control Directo (Inspección In Situ) y el Control Indirecto (Inspección Extra Situ).

LA ORGANIZACIÓN INTERNACIONAL DE ENTIDADES FISCALIZADORAS SUPERIORES (INTOSAI)

Provee un marco de trabajo institucionalizado a las Entidades Fiscalizadoras Superiores, para promover el desarrollo y la transferencia de conocimientos, la mejora de la auditoría del sector público en todo el mundo y aumentar las capacidades profesionales, la presencia e influencia de sus miembros en sus respectivos países. Las Entidades Fiscalizadoras Superiores son autoridades nacionales con responsabilidad dentro de su sistema constitucional, para auditar actividades financiadas con fondos públicos. El intercambio de conocimientos entre miembros de la INTOSAI y los hallazgos y puntos de vista resultantes son una garantía de que la auditoría del sector público mejora continuamente.

La INTOSAI emite dos tipos de normas profesionales: las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI) y las Directrices de la INTOSAI para la Buena Gobernanza (INTOSAI GOV)

Las ISSAI y las INTOSAI GOV transmiten los principios reconocidos de manera general y experiencias profesionales compartidas de la comunidad internacional de Entidades Fiscalizadoras Superiores.

Todas las ISSAI e INTOSAI GOV son desarrolladas y mantenidas de acuerdo con el Debido Proceso para las Normas Profesionales de la INTOSAI y emitidas tras la aprobación definitiva por parte de todas las Entidades Fiscalizadoras Superiores reunidas en el Congreso de la INTOSAI (INCOSAI).

NORMAS INTERNACIONALES DE LAS ENTIDADES FISCALIZADORAS SUPERIORES (ISSAI)

International Standard of Supreme Audit Institutions se estableció formalmente en el 2007 y refleja la ambiciosa visión de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI) de proveer a sus miembros y partes interesadas, un marco de trabajo para normas de auditoría, profesional y de alta calidad.

Las ISSAI tienen el objetivo de salvaguardar independencia y efectividad de la actividad auditora, y apoyar a los miembros de la INTOSAI en el desarrollo de su propio enfoque profesional en función de su mandato. La primera serie completa de ISSAI fue puesta en marcha en el XX Congreso de Johannesburgo, Sudáfrica, en 2010. A través de la Declaración de Sudáfrica.

CAPÍTULO III. MARCO METODOLÓGICO

La metodología del proyecto incluye el tipo y nivel de investigación, unidad de análisis, procedimientos objetivos, operacionalización de las variables, consideraciones éticas toda la información referente a técnicas y procedimientos que serán utilizados para llevar a cabo la indagación. Es el "cómo" se realizó el estudio para responder al problema planteado.

TIPO DE INVESTIGACIÓN

El objetivo general de investigación del presente proyecto de Trabajo de Grado de Maestría está orientado al desarrollo de un Modelo de Evaluación Integral de Sistema de Información de Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana, la cual como indica Yáber y Valarino (2003), su tipo de investigación investigación y desarrollo, tiene como propósito indagar sobre necesidades del ambiente interno o entorno de una organización, para luego desarrollar una solución que pueda aplicarse en una empresa o mercado. El problema podría plantearse como un enunciado interrogativo que relaciona el producto o servicio a desarrollar y la necesidad por atender. La cual tiene como propósito resolver un problema práctico.

Para esta investigación fue necesario desarrollar los requerimientos técnicos, evaluar el nivel de brecha, formular dicho modelo y aplicar una prueba de concepto del mismo.

DISEÑO DE LA INVESTIGACIÓN

Altuve y Rivas (1998), aseguran que el diseño de una investigación es una estrategia general que adopta el investigador como forma de abordar un problema

determinado, que permite identificar los pasos que deben seguir para efectuar su estudio.

Según el autor Arias (2012), define: La investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos (datos primarios), sin manipular o controlar variable alguna, es decir, el investigador obtiene la información pero no altera las condiciones existentes. De allí su carácter de investigación no experimental.
Según Hernández, Fernández y Baptista (2003), definen el diseño de investigación no experimental como la investigación que se realiza sin manipular deliberadamente variables y en los que solo se observan los fenómenos en su ambiente natural para después analizarlos.

Para Sampieri (2003), el diseño no experimental se divide tomando en cuenta el tiempo durante se recolectan los datos, diseño Transversal, donde se recolectan datos en un solo momento, en un tiempo único, su propósito es describir variables y su incidencia de interrelación en momento dado.

Para fines de estudio será de campo no experimental transversal, debido a que se recolectaran datos en un tiempo sin intervenir en el ambiente en que se desarrollan, por lo que no habrá manipulación de variables.

UNIDAD DE ANÁLISIS

Según Sampieri (2003), la unidad de análisis son los sujetos que van a ser medidos, para este estudio se interactuó con las unidades funcionales y los empleados activos que correspondan a la entidad mayor o representativa que estén a cargo de la Unidad de Prevención y Legitimación de Capitales Banca Pública en Venezuela, para ellos se respetara los códigos de éticas y las normas de confidencialidad.

Unidad de análisis y objeto de estudio la Banca Pública venezolana, con juicio de experto de personal clave en las distintas áreas asociadas a la Unidad de Prevención y Legitimación de Capitales, por cumplir los estándares a nivel internacionales, que se incluye Basilea y el GAFI.

PROCEDIMIENTOS OBJETIVOS

Objetivo Especifico 1: Identificar los requerimientos técnicos y funcionales de un sistema de Administración de Riesgo de Legitimación de Capitales en la banca pública venezolana. A través de observación directa a la Unidad de Legitimación, revisión de leyes y normativas exigidas, usando marco lógico y metodología Zopp, con el fin de verificar los procesos y las necesidades en la unidad en estudio.

Objetivo Especifico 2: Evaluar el nivel de brecha de los requerimientos de trazabilidad en el Sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana. Para esto fue necesario interactuar con el personal de la Unidad de Legitimación y Prevención de Legitimación de Capitales, de la Banca Pública, con el fin de precisar la problemática existente en los procesos, clientes internos y calidad de servicios. Además de emplear los estándares especializados en el área.

Objetivo Especifico 3: Formular un modelo de evaluación integral del sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana. Dar resultados de los procesos, la actividad del personal y la posible falla en sistemas internos inadecuados o defectuosos alineados al modelo de ingeniería del software y los principios de Basilea. De igual manera se realizó consultas a expertos en el área.

Objetivo Especifico 4: Aplicar una prueba de concepto del modelo de evaluación integral del sistema Información Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana, a través de pruebas de caja negra y caja

blanca con el fin de precisar las oportunidades de mejoras, la necesidad de cambio, que permitieron optimizar el proceso y minimizar los riesgos presentes en la banca pública venezolana en el área de Legitimación de Capitales y Financiamiento al Terrorismo.

FASES DE LA INVESTIGACIÓN

La investigación se realizó por fases, se dividió la ejecución del proyecto de grado en 5 fases, las 4 primeras fases es el desarrollo de los cuatros objetivos específicos planteados, y la fase 5 corresponde desde el cierre del proyecto hasta su consignación.

Fase 1 Resumen ejecutivo de la identificación de los requerimientos técnicos y funcionales del sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.

Fase 2 Resumen de la evaluación del nivel de brecha de los requerimientos de trazabilidad en el Sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.

Fase 3 Modelo de evaluación integral del sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Publica Venezolana.

Fase 4 Evaluación de la prueba de concepto del modelo de evaluación integral del sistema Información Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.

Fase 5 Cierre e Impresión de documentos y defensa del proyecto.

OPERACIONALIZACIÓN DE LAS VARIABLES

Bavaresco (1996), se refiere a las variables cómo las diferentes condiciones, cualidades características o modalidades que asumen los objetos en estudio desde el inicio de la investigación. Constituyen la imagen inicial del concepto dado dentro del marco. A tal efecto, se establecen la siguiente variables e indicadores que se conceptualizan más adelante. Otro elemento que se definirá en esta investigación fueron los indicadores, que como señala Altuve (1.990), son una definición que asigna significado a una construcción conceptual de la variable, al especificar actividades u operaciones necesarias para medirlas. Ver tabla 6 anexa.

.

Tabla 6. Operacionalización de las variables de la investigación.

Objetivo General	ObjetivosEspecíficos	Variable	Dimension	Indicadores	Área de aplicación	Técnica	Fuente de la Investigación
Desarrollar un Modelo de Evaluación Integral del Sistema de Información Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.	Identificar los requerimientos técnicos y funcionales de un sistema de Administración de Riesgo de Legitimación de Capitales en la banca pública venezolana.	Riesgo	Legitimación Transacciones Cliente Operaciones pasivas y activas	Riesgo Legitimación de Capitales	Procesos Internos Usuarios	Observación Directa Process Mapping Estándares IEEE Juicio de Experto	Fuente Secundaria Fuentes Públicas SUDEBAN GAFI Basilea I, II y III Base de datos Académica Normativa legal vigente
	Evaluar el nivel de brecha de los requerimientos de trazabilidad en el Sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.			Riesgo Legitimación de Capitales	Procesos usuarios Calidad de servicio		Banco de Venezuela SUDEBAN Basilea I,II y III INTOSAI ISSAI GAFI Base de datos Académica Normativa legal vigente
	Formular un modelo de evaluación integral del sistema de Administración de Riesgo de Legitimación de Capitales.			Riesgo Legitimación de Capitales	Resultado de los procesos Actividad del personal Sistemas internos	Business Intelligence E-commerce	Fuente Secundaria: ISSAI e INTOSAI y los principios de Basilea I,II y III (Normas internacionales) Base de datos Académica Normativa legal vigente
	Evaluar la prueba de concepto del modelo de evaluación integral del sistema Información Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.			Resultados obtenidos	Proceso Interno (Aprendizaje, crecimiento) Oportunidades de mejoras Necesidad de cambio	Pruebas de caja negra y caja blanca	Fuente secundaria: Evaluación de acuerdo a Basilea I, Basilea II Y Basilea III Base de datos Académica Normativa legal vigente

CONSIDERACIONES ÉTICAS Y LEGALES

El presente trabajo de investigación se trabajara de acuerdo:

Código de ética profesional vigente del Colegio de Ingenieros de Venezuela (1996), el investigador debe tomar en cuenta:

- Actuar en cualquier forma que tienda a menoscabar el honor, la responsabilidad y aquellas virtudes de honestidad, integridad y veracidad que deben servir de base a un ejercicio cabal de la profesión.
- Utilizar estudios, proyectos, planos, informes u otros documentos, que no sean el dominio público, sin la autorización de sus autores y/o propietarios.

.

CAPÍTULO IV. MARCO REFERENCIAL ORGANIZACIONAL

FUNDAMENTOS ORGANIZACIONALES

La Banca Pública surge en Venezuela por la necesidad de la intermediación social y por la inestabilidad bancaria existente influenciada principalmente por la falta de estabilidad política, la mayor parte de la banca sólo concedía préstamos al sector gubernamental y participaba como ente de recaudación aduanera.

En el gobierno de Antonio Guzmán Blanco (1870-1887) se sentaron las bases legales para el establecimiento de bancos en Venezuela.

En la Dictadura de Juan Vicente Gómez en 1928 que se crean dos bancos públicos especializados; el 13 de junio el Banco Agrícola y Pecuario, para incentivar el sector agrícola y el 30 de junio el Banco Obrero para impulsar la construcción de viviendas populares. En el gobierno de Eleazar López Contreras (1935-1941) se modernizó la Banca con la creación del Banco Industrial de Venezuela para financiar e impulsar el desarrollo industrial.

En 1989 en el Gobierno de Carlos Andrés Pérez se desató en Venezuela una gran crisis bancaria, se desplomaron varios bancos del Sector Privado, entre ellos el Banco más antiguo del país, el Banco de Maracaibo. La crisis es superada en el año 1996.El 3 de julio de 2009, se renacionaliza el Banco Venezuela para fortalecer el sistema bancario público nacional e impulsar las políticas de desarrollo económico y social. A partir del 21 de septiembre de 2009 pasa a ser Administrado por el Estado.

Tabla 7. Banca pública venezolana

Entidad Financiera	Visión	Misión	Cantidad de agencias	Banca en línea
Banco Bicentenario del Pueblo, de la Clase Obrera, Mujer y Comunas	La entidad está orientada a la atención de los trabajadores venezolanos, donde podrán tramitar créditos hipotecarios, financiamientos para formar cooperativas, pedir microcréditos y renovarlos. Las empresas y trabajadores que depositen sus prestaciones sociales y colectivas en la institución, contarán con un buen servicio, préstamos especiales y apoyo financiero.	El primer banco socialista en Venezuela, institución financiera comprometida con la clase obrera trabajadora, cuyo objetivo principal es fortalecer el desarrollo socio-productivo de la nación.	542	Si http://www.bicentenariobu.com/paginas/detalle/nosotros_historia.php
Banco de Venezuela	El Banco de Venezuela expande su horizonte hacia una visión incluyente, amplia y democrática de los servicios financieros, como una vía para llevar bienestar y	Misión la consolidación como la mejor institución de servicios financieros en Venezuela, mediante un modelo de gestión orientado a la creación permanente de valor para nuestros clientes, nuestra empleada y para el país. Ofrece amplia gama de	419	Si bancodevenezuela.com/?bdv=link_inicio

	felicidad al pueblo venezolano. Atención bancaria permitiendo lograr la necesaria democratización de los servicios financieros, asumiendo que la meta es continuar siendo un banco líder, pero consciente de que el liderazgo es una responsabilidad y un compromiso.	servicios para facilitar las operaciones financieras. Tiene a disposición un amplio portafolio de productos que permitirá la movilidad de las cuentas los 365 días del año		
Banco del Tesoro	Ser la institución bancaria del Estado reconocida por la integridad, excelencia y compromiso de nuestra gente, con tecnología de punta, para proveer servicios de calidad, contribuyendo al desarrollo nacional.	Concebida para proveer servicios confiables, oportunos y rentables a fin de satisfacer las necesidades de nuestros clientes e impulsar los planes estratégicos del País.	93	Si http://www.bt.gob.ve/#/node/1
Banco de Desarrollo Económico y Social de Venezuela	financiamiento de proyectos relacionados con la modernización de la infraestructura social, programas de cooperación internacional e	**Estimular la inversión privada en zonas de bajos ingresos**	1	No

	innovación tecnológica			
Banco de desarrollo de la mujer	Ser un medio para la consolidación de la economía socialista, popular, solidaria y ambientalmente sustentable, con igualdad y equidad de género, donde las mujeres son parte esencial de la vida socio-económica del País, en una sociedad justa y amante de la paz.	**Conceder créditos, microcréditos y otros servicios financieros a grupos y cooperativas de mujeres, sobre todo las de las clases socioeconómicas más desposeídas**		No http://www.banmujer.gob.ve/

Fuente: (Resumen banca pública, 2017)

CAPÍTULO V. Identificación de los requerimientos técnicos y funcionales de un sistema de Administración de Riesgo de Legitimación de Capitales en la banca pública venezolana.

Para identificar los requerimientos técnicos y funcionales fue necesaria la revisión de las leyes vigente en la banca pública venezolana:

- Ley Orgánica Contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDO/FT), publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 39.912 de fecha 30 de abril de 2012.Ley Orgánica de Drogas, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 39.546 de fecha 05 de noviembre de 2010.
- Ley de Instituciones del Sector Bancario, publicada el martes 02 de diciembre de 2014 en la Gaceta Oficial Extraordinaria Nº 6.154. Resolución Nº 119.10, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 39.388 del 9 de marzo de 2010, la cual establece las normas relativas a la Administración y Fiscalización de los Riesgos Relacionados con los Delitos de Legitimación de Capitales y Financiamiento al Terrorismo aplicables a las Instituciones reguladas por la Superintendencia de Bancos y otras Instituciones Financieras.
- Ley Orgánica de Drogas, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 39.546 de fecha 05 de noviembre de 2010.
- Resolución Nº 119.10, publicada en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 39.388 del 9 de marzo de 2010, la cual establece las normas relativas a la Administración y Fiscalización de los Riesgos Relacionados con los Delitos de Legitimación de Capitales y Financiamiento al Terrorismo aplicables a las Instituciones reguladas por la Superintendencia de Bancos

Con la intención de cumplir la normativa señalada y mitigar los distintos riesgos asociados a la Legitimación de Capitales y el Financiamiento al Terrorismo, se desarrolla políticas, procedimientos y medidas apropiadas, suficientes y eficaces, orientadas a identificar, evaluar y aplicar correctivos para reducir la posibilidad de que en la realización de cualquier operación financiera, sea utilizado como medio para ocultar el origen, propósito y destino de capitales ilícitos, o para desviar fondos de cualquier naturaleza hacia el financiamiento de grupos o actividades terroristas.

La Legitimación de Capitales, ha sido estudiada muy a fondo, y se han definido unas etapas que permiten entender como la Delincuencia Organizada ha estructurado sus actuaciones al pasar de los años, para ingresar a los sistemas financieros. **Colocación:** Procedimiento utilizado por la delincuencia organizada para deshacerse físicamente del dinero derivado de actividades ilegales, especialmente a través de los bancos, mediante altos ingresos de Fondos, así como en operaciones al menudeo, al por menor o estructuradas. Ejemplo de esto, pueden observarse en la figura 5. Depósitos bancarios en cuentas corrientes y ahorros; depósitos en cuentas bancarias, para ingresar el dinero a la banca.

En la figura 5 se muestra el proceso de legitimación desde la Colocación del dinero en el sistema financiero en este caso en la oficina de la entidad bancaria, iniciando así el proceso de legitimación de capitales de los fondos ilegales al sistema financiero. Procesamiento es realizar múltiples operaciones financieras, con el fin de eliminar todo rastro del origen.

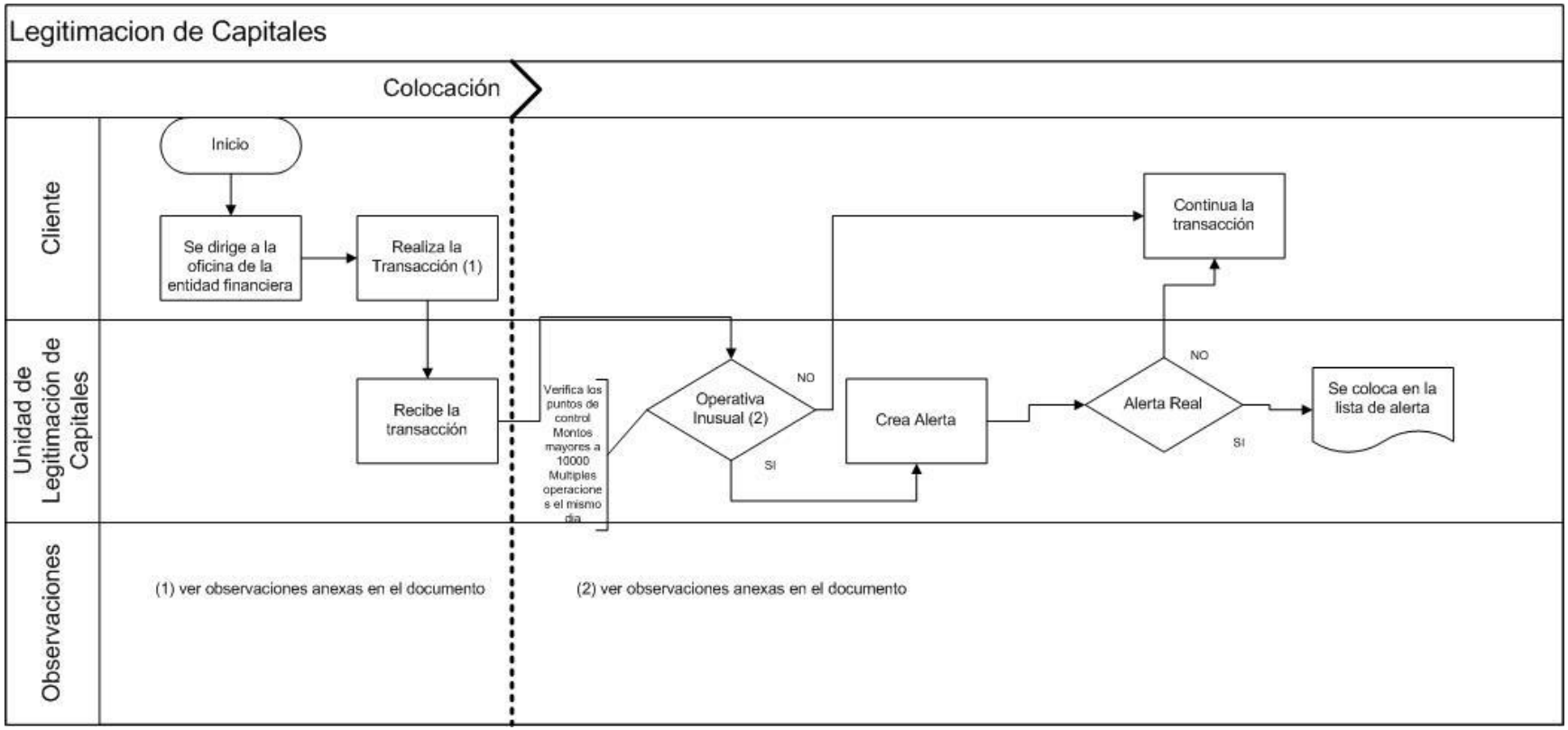

Figura 5. Legitimación de Capitales

Fuente: Caja venezolana de valores, 2017.

En las observaciones se puede identificar:

OBSERVACION 1: Según GAFI (2012) Los países deben identificar, evaluar y entender sus riesgos de lavado de activos/financiamiento del terrorismo, y deben tomar medidas, incluyendo la designación de una autoridad o mecanismo para coordinar acciones para evaluar los riesgos, y aplicar recursos encaminados a asegurar que se mitiguen eficazmente los riesgos. Con base en esa evaluación, los países deben aplicar un enfoque basado en riesgo (EBR) a fin de asegurar que las medidas para prevenir o mitigar el lavado de activos y el financiamiento del terrorismo sean proporcionales a los riesgos identificados. Este enfoque debe constituir un fundamento esencial para la asignación eficaz de recursos en todo el régimen antilavado de activos y contra el financiamiento del terrorismo (ALA/CFT) y la implementación de medidas basadas en riesgo en todas las Recomendaciones del GAFI.

Resolución Nro119.110 emitida por Sudeban los regulados por la SUDEBAN, son susceptibles de ser utilizados por personas que realicen actividades ilícitas relacionadas con los delitos de delincuencia organizada, debido a que existen diversas operación es, productos y servicios de carácter financiero, que pueden servir de instrumento para la LC/FT.

El GAFI indica la debida diligencia sobre los clientes y la conservación papeles.

OBSERVACIÓN 2: Según recomendación del GAFI (2012) los países deben desarrollar e implementar procedimientos que se conozcan públicamente para presentar solicitudes al Consejo de Seguridad a fin de excluir de las listas a personas y entidades designadas, que, en opinión del país, no satisfacen o ya no satisfacen los criterios de la designación. Una vez que el Comité de Sanciones correspondiente haya removido a la persona o entidad, la obligación de congelamiento deja de existir. Estos procedimientos y criterios deben estar de conformidad con las directrices o procedimientos aplicables aprobados por el Consejo de Seguridad en virtud de la Resolución 1730 (2006) y las resoluciones

sucesoras, incluyendo las del mecanismo de Punto Focal creado dentro de esa resolución. Los países deben permitir a las personas y entidades listadas presentar una petición de remoción en el Punto Focal para el proceso de remoción de la lista establecido en virtud de la Resolución 1730 (2006) o deben informar a las personas o entidades designadas que presenten directamente la solicitud al Punto Focal.

Según GAFI exigirse a las instituciones financieras y las APNFD que tomen medidas apropiadas para identificar y evaluar sus riesgos de lavado de activos y financiamiento del terrorismo (para los clientes, países o áreas geográficas; y productos, servicios, transacciones o canales de envío). Éstas deben documentar esas evaluaciones para poder demostrar sus bases, mantener estas evaluaciones actualizadas, y contar con los mecanismos apropiados para suministrar información acerca de la evaluación del riesgo a las autoridades competentes y los OAR.

Delito de lavado de activos: Los países deben tipificar el lavado de activos en base a la Convención de Viena y la Convención de Palermo. Los países deben aplicar el delito de lavado de activos a todos los delitos graves, con la finalidad de incluir la mayor gama posible de delitos determinantes.
Los países deben tipificar el financiamiento del terrorismo en base al Convenio Internacional para la Represión de la Financiación del Terrorismo, y deben tipificar no sólo el financiamiento de actos terroristas, sino también el financiamiento de organizaciones terroristas y terroristas individuales, aún en ausencia de un vínculo con un acto o actos terroristas específicos. Los países deben asegurar que tales delitos sean designados como delitos determinantes del lavado de activos para las personas o entidades con el mismo nombre o un nombre similar al de las personas o entidades designadas, que se ven afectadas por descuido por un mecanismo de congelamiento (es decir, un falso positivo), los países deben desarrollar e implementar procedimientos que se conozcan públicamente para descongelar los fondos u otros activos de dichas personas o entidades, oportunamente, en cuanto se realice la verificación de que la persona o entidad involucrada no es una persona o entidad designada.

OBSERVACIÓN 3: Según recomendación del GAFI (año 2012), exigirse a las instituciones financieras y las APNFD que tomen medidas apropiadas para identificar y evaluar sus riesgos de lavado de activos y financiamiento del terrorismo (para los clientes, países o áreas geográficas; y productos, servicios, transacciones o canales de envío). Éstas deben documentar esas evaluaciones para poder demostrar sus bases, mantener estas evaluaciones actualizadas, y contar con los mecanismos apropiados para suministrar información acerca de la evaluación del riesgo a las autoridades competentes y los OAR.

Análisis de brecha

Para el análisis de brecha se hizo el marco lógico de la mano con la metodología Zopp (2014), el nombre del método proviene de la denominación alemana ziel orientierte projekt planung (planeación de proyectos orientada a objetivos. Por medio de la tabla se permite presentar de forma sistemática los requerimientos exigidos por GAFI, la situación actual, el escenario ideal frente a la información plateada por el GAFI, las normativas y exigencias por parte de sudeban.

En la tabla 8 se muestra un análisis del requerimiento técnico y funcional GAFI, la situación actual en la banca pública, la situación ideal que llevaría al aplicar el modelo, lo solicitado por el SUDEBAN y las observaciones. En las observaciones se muestra la brecha existente en lo que actualmente se encuentra implementado y lo solicitado en el ámbito legal de la SUDEBAN.

Tabla 8. Análisis de brecha

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
Los países deben identificar, evaluar y entender sus riesgos de lavado de activos/financiamiento del terrorismo, y deben tomar medidas, incluyendo la designación de una autoridad o mecanismo para coordinar acciones para evaluar los riesgos, y aplicar recursos encaminados a asegurar que se mitiguen eficazmente los riesgos. Con base en esa evaluación, los países deben aplicar un enfoque basado en riesgo (EBR EBR) a fin de asegurar que las medidas para prevenir o mitigar el lavado de activos y el financiamiento del terrorismo sean proporcionales	No cuentan con una herramienta para realizar el enfoque basado en riesgo. Aunque tienen una unidad de legitimación de capitales con el fin de encaminar las diferentes acciones para cumplir con los requerimientos exigidos por la SUDEBAN.	Obtener de manera automatizada información con el fin reportar actividades sospechosas de legitimación de Capitales y Financiamiento del Terrorismo, basado en riesgo con el fin de detectar en el momento de la operación y así poder alertar a tiempo.	Diseño e implementación del Sistema Integral de Administración de Riesgos de LC/FT Los Sujetos Obligados, de acuerdo con la naturaleza y complejidad de sus negocios, productos y servicios financieros, al volumen de operaciones, a la región geográfica donde actúan, a la tecnología disponible y en concordancia con el nivel de sus riesgos de LC/FT y en cumplimiento de las disposiciones legales que rigen la materia y las presentes Normas; deben formular, adoptar, implementar y desarrollar, un “Sistema Integral de Administración de Riesgos de Legitimación de Capitales y del Financiamiento al Terrorismo”	Es prioritario la revisión obligatoria de la operativa sensible manteniendo como características la descentralización (para todas las oficinas o dependencias del banco) y centralización para la unidad de prevención y control de legitimación de capitales, que agrupe todos los productos que maneja el banco para cada uno de los clientes tales como: cuenta corriente, ahorro, fidecomiso, tarjetas de crédito y

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
a los riesgos identificados. Este enfoque debe constituir un fundamento esencial para la asignación eficaz de recursos en todo el régimen anti lavado de activos y contra el financiamiento del terrorismo (ALA/CFT) y la implementación de medidas basadas en riesgo en todas las Recomendaciones del GAFI. Cuando los países identifiquen riesgos mayores, éstos deben asegurar que sus respectivos regímenes ALA/CFT aborden adecuadamente tales riesgos. Cuando los países identifiquen riesgos menores, éstos pueden optar por permitir medidas				operaciones con tarjetas de crédito del exterior utilizada por puntos, operaciones con moneda extranjera, operaciones realizadas, banca corresponsal, banca por internet, plazo fijo, créditos, operaciones en cajeros automáticos del banco

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
simplificadas para algunas Recomendaciones del GAFI bajo determinadas condiciones.				
Los países deben contar con políticas ALA/CFT a escala nacional, que tomen en cuenta los riesgos identificados, las cuales deben ser sometidas a revisión periódicamente, y deben designar a una autoridad o contar con un mecanismo de coordinación o de otro tipo que sea responsable de dichas políticas. Los países deben asegurar que, las autoridades que hacen las políticas, la Unidad de Inteligencia Financiera (UIF), las autoridades del orden público, los supervisores y otras autoridades competentes relevantes, tanto a nivel de formulación de políticas como	No cuentan con los mecanismos necesarios para reportar en tiempo real las diferentes transacciones que puedan estar asociadas a legitimación de capitales y financiamiento al terrorismo.	Establecer acuerdos con otros organismos con el fin de ver en tiempo real situaciones que puedan estar asociadas a legitimación de capitales y financiamiento al terrorismo con el propósito de actuar en el momento oportuno y tratar de prevenir las distintas situaciones que pueden ser lamentables para la nación.	La SUDEBAN, de conformidad con el artículo 136 de la Constitución de la República Bolivariana de Venezuela, establecerá Acuerdos de Cooperación con otros Organismos de Control, Supervisión, Fiscalización y Vigilancia contemplados en la LOCDO, a fin de implementar los procedimientos mediante los cuales la UNIF recibirá los Reportes de Actividades Sospechosas y otra información periódica necesaria para realizar los análisis e investigación administrativa que se requieran, según lo establecido en el	

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
operativo, cuenten con mecanismos eficaces establecidos que les permita cooperar y, cuando corresponda, entablar entre sí una coordinación a nivel interno en el desarrollo e implementación de políticas y actividades para combatir el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva.			artículo 51 de la LOCDO.	
Delito de lavado de activos Los países deben tipificar el lavado de activos en base a la Convención de Viena y la Convención de Palermo. Los países deben aplicar el delito de lavado de activos a todos los delitos graves, con la finalidad de incluir la mayor gama posible de delitos determinantes.	Se encargan de enviar informes a la SUDEBAN sobre los posibles casos de legitimación de capitales y financiamiento al terrorismo y ellos se encargaran de reportar y	Se envía en línea la información relacionada con actividades ilícitas al ente pertinente, de manera rápida y eficaz con el fin que las autoridades investiguen y ejecuten las acciones pertinentes.	Que los entes regulados por la SUDEBAN, son susceptibles de ser utilizados por personas que realicen actividades ilícitas relacionadas con los delitos de delincuencia organizada, debido a que existen diversas operaciones, productos y servicios decarácter financiero, que	La convención de viena representa un verdadero punto de inflexión en la política a seguir en el marco de la lucha contra el lavado de capitales ya que trato de darle carácter jurídico

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
Decomiso y medidas provisionales Los países deben adoptar medidas similares a las establecidas en la Convención de Viena, la Convención de Palermo y el Convenio Internacional para la Represión de la Financiación del Terrorismo, incluyendo medidas legislativas, que permitan a sus autoridades competentes congelar o incautar y decomisar lo siguiente, sin perjuicio de los derechos de terceros de buena fe: (a) bienes lavados, (b) producto de, o instrumentos utilizados en, o destinados al uso en, delitos de lavado de activos o delitos determinantes , (c) bienes que son el producto de, o fueron utilizados en, o que se pretendía utilizar o	el ente encargado verificara la información suministrada.		pueden servir de instrumento para la LC/FT, lo cual vulnera los procesos económicos, políticos y sociales del país y de dichas Instituciones,afectando su credibilidad y legitimidad en el contexto nacional e internacional. Recibir y analizar los reportes internos de actividades sospechosas enviados por lasdiferentes dependencias del Sujeto Obligado a los fines de determinar, previoanálisis e investigación, si hay indicios suficientes para clasificar los hechos otransacciones como actividades sospechosas. No es responsabilidad de las Instituciones Financieras el determinar el tipo deactividad criminal que se esté realizando, el	para poder sancionar a personas que estén incurriendo en el delito

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
asignar para ser utilizados en el financiamiento del terrorismo, actos terroristas u organizaciones terroristas, o (d) bienes de valor equivalente. Estas medidas deben incluir la autoridad para: (a) identificar, rastrear y evaluar bienes que están sujetos a decomiso; (b) ejecutar medidas provisionales, como congelamiento y embargo, para prevenir manejos, transferencias o disposición de dichos bienes; (c) adoptar medidas que impidan o anulen acciones que perjudiquen la capacidad del Estado para congelar o embargar o recuperar los bienes sujetos a decomiso; y (d) tomar las medidas de investigación apropiadas.			deber del Sujeto Obligado es reportarla actividad sospechosaoportunamente a la UNIF. Las autoridades de investigación penal examinarán el asunto con mayordetenimiento y determinarán si existe un enlace con el financiamiento alterrorismo.	
Delito de Financiamiento del Terrorismo	Los mecanismos	Penalizar adecuadamente el	por disposición de la Ley Orgánica	

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
Sanciones financieras dirigidas relacionadas al terrorismo y al financiamiento del terrorismo Organizaciones sin fines de lucro	actuales no permiten dar la información en tiempo real, retrasándose la notificación y actuando de forma ineficaz para informar los posibles ataques que puedan presentarse.	financiamiento del terrorismo Establecer y aplicar procedimientos apropiados para identificar y congelar activos de terroristas. Aplicar directrices oportunas para la ejecución de la política de Diligencia Debida sobre los clientes de todos los sectores. Este punto, entendemos, significa el obligatorio cumplimiento del programa "Conozca al cliente", no sólo en las instituciones financieras, sino también en casinos y salas de bingo, inmobiliaria y compravent	Contra la Delincuencia Organizada (en adelante LOCDO), dichas Instituciones adquieren obligaciones legales que les dan posición de garantes; así como, obligaciones de diligencia debida y buena fe, para mitigar los riesgos relacionados con la comisión de los delitos de LC/FT, tipificados en los artículos 4, 5 y 7 de la citada Ley Orgánica. Art.67 Los Sujetos Obligados aplicarán los procedimientos siguientes para detectar actividades de financiamiento al terrorismo: 1. Aplicar procedimientos de monitoreo sobre las transacciones con países o áreas geográficas según listas emanadas del Consejo de Seguridad de Naciones Unidas,dondeindividuos,	

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
		a de bienes inmuebles, empresas dedicadas a la construcción, entre otros sujetos obligados establecidos en el artículo 42 de la Ley Orgánica contra la Delincuencia Organizada.	organizaciones o países en particular fuesen sometidos asanciones por el financiamiento al terrorismo. 2. Monitoreo que permita identificar transacciones relacionadas con personasnaturales o jurídicas que han sido identificadas en otras jurisdicciones comoelementos relacionados con organizaciones o actividades terroristas o sufinanciamiento. 3. Procedimientos de control interno y señales de alerta basados en las tipologíasdetectadas y difundidas por las autoridades nacionales u otras jurisdiccionesrelacionadas con el financiamiento de actividades terroristas.	
Medidas preventivas Leyes sobre el secreto de las instituciones financieras Los países deben asegurar que las	Actitud proactiva y diligente ante las autoridades de la Administración de	Actitud proactiva y diligente ante las autoridades de la Administración de	Artículo 83.- Obligación de Colaborar con el Ejecutivo Nacional Es obligación de los Sujetos Obligados, colaborar con el	

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
leyes sobre el secreto de la institución financiera no impidan la implementación de las Recomendaciones del GAFI	Justicia en contra de los delitos, el secreto bancario, secreto profesional o confidencialidad debida, no esobjetable las solicitudes de información formuladas por las autoridades ni a losreportes que efectúe el Sujeto Obligado por propia iniciativa ante una sospecha.	Justicia en contra de los delitos, el secreto bancario, secreto profesional o confidencialidad debida, no escriticables las solicitudes de información formuladas por las autoridades ni a losreportes que efectúe el Sujeto Obligado por propia iniciativa ante una sospecha.	Ejecutivo Nacional atendiendolos requerimientos expresos de las autoridades y evidenciando una actitud proactiva ydiligente ante las autoridades de la Administración de Justicia en contra de los delitosde LC/FT. El secreto bancario, secreto profesional o confidencialidad debida, no es oponible a las solicitudes de información formuladas por las autoridades ni a los reportes que efectúe el Sujeto Obligado por propia iniciativa ante una sospecha de LC/FT; tal como lo prevé el artículo 51 de la LOCDO.	
Debida diligencia y mantenimiento de registros Debe prohibirse a las instituciones financieras que mantengan cuentas anónimas o cuentas con nombres	Están trabajando en la política conoce a tu cliente con el fin de dar cumplimiento a la resolución	Automatizar el registro del cliente con el fin de mantener siempre en línea el expediente del cliente y realizar constante	Artículo 35.- Registros Individuales de los Clientes Los Sujetos Obligados deberán establecer registros individuales de cada uno de sus	

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
obviamente ficticios. Debe exigirse a las instituciones financieras que emprendan medidas de Debida Diligencia del Cliente (DDC) cuando: (i) establecen relaciones comerciales; (ii) realizan transacciones ocasionales: (i) por encima del umbral aplicable designado (USD/EUR 15,000); o (ii) están ante transferencias electrónicas en las circunstancias que aborda la Nota Interpretativa de la Recomendación 16; (iii) existe una sospecha de lavado de activos o financiamiento del terrorismo; o (iv) la institución financiera tiene dudas sobre la veracidad o idoneidad de los datos de identificación sobre el cliente	119-10 de la SUDEBAN	monitoreo de las transacciones y el uso de las cuentas del cliente.	clientes con el fin de obtener y mantener actualizada la información necesaria paradeterminar fehacientemente su identificación y las actividades económicas a las quese dedican y adoptar parámetros de segmentación, a los efectos de definir su perfilfinanciero de modo que dicho perfil facilite la identificación de las operacionesinusuales o sospechosas. Artículo 36.- Apertura de Cuentas Bancarias por primera vez Para abrir cuentas bancarias o financieras de cualquier tipo por primera vez en una Institución Financiera, será requisito indispensable realizar una entrevista personal con 25	

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
obtenidos previamente. El principio de que las instituciones financieras deben llevar a cabo la DDC debe plasmarse en ley. Cada país puede determinar cómo impone obligaciones específicas de DDC, ya sea mediante ley o medios coercitivos. Mantenimiento de registros Debe exigirse a las instituciones financieras que mantengan, por un período de al menos cinco años, todos los registros necesarios sobre las transacciones, tanto locales como internacionales, para que éstas puedan cumplir con rapidez con las peticiones de información solicitadas por las autoridades competentes. Estos registros tienen que ser suficientes para permitir la			el solicitante o con la persona autorizada por éste, incluyendo aquellas que posteriormente serán manejadas mediante los servicios de “Banca Virtual” o “Banca a Distancia”, tales como los de “Banco en Casa” o “Banca a Través de Internet” (Home Banking o Internet Banking), y “Servicios de Banca en Línea” (On Line Banking Services). Artículo 37.- Documentos para la identificación del cliente La identificación del cliente se realizará a través de la cédula de identidad laminadapara personas naturales venezolanas y extranjeras residentes en el país, y pasaportepara personas naturales extranjeras no residentes.	

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
reconstrucción de transacciones individuales (incluyendo los montos y tipos de moneda involucrada, de haber alguna) de manera tal que se ofrezca evidencia, de ser necesario, para el enjuiciamiento de una actividad criminal			En el caso de personas jurídicas domiciliadas en el país, la identificación se efectuará a través del Registro de Información Fiscal (RIF) expedido por el Servicio Nacional Integrado de Administración Aduanera y Tributaria (SENIAT) y las copias certificadasde los documentos constitutivos de la empresa, sus estatutos sociales ymodificaciones posteriores, debidamente inscritos en el Registro Mercantil o en elRegistro Civil.	
Regulación y supervisión de las instituciones financieras Los países deben asegurar que las instituciones financieras estén sujetas a una regulación y supervisión adecuadas y que implementen	La institución financiera esta sujeta a una regulación y supervisión adecuada y está en revisión constante	Las instituciones financieras deben estar estén sujetas a una regulación y supervisión constante con el fin que implemente	la SUDEBAN tendrá en su estructura organizativa la Unidad Nacional de Inteligencia Financiera (en adelante UNIF); Unidad de carácter administrativo, que según los estándares y	

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
eficazmente las Recomendaciones del GAFI. Las autoridades competentes deben tomar las medidas legales o normativas necesarias para prevenir que los criminales o sus cómplices tengan, o sean el beneficiario final de, o que tengan una participación significativa o mayoritaria en, o que ostenten una función administrativa en una institución financiera. Los países no deben aprobar el establecimiento u operación continuada de bancos pantalla. En el caso de las instituciones financieras sujetas a los Principios Centrales, las medidas de regulación y supervisión que se aplican para propósitos prudenciales y que son relevantes también para el	del ente supervisor la SUDEBAN para cumplir normativas.	n eficazmente las Recomendaciones del GAFI.	mejores prácticas definidas en los tratados y convenios suscritos por nuestro País y por las organizaciones internacionales a los cuales la República Bolivariana de Venezuela se encuentra adscrita, entre ellos la Organización de Estados Americanos y la Comisión Interamericana para el Control de Abuso de Drogas (OEA/CICAD), el Grupo de Acción Financiera del Caribe (GAFIC) y el Grupo Egmont, la definen como una organización centralizadora que recibe, evalúa ytramita los informes periódicos y de actividades sospechosas provenientes de lasinstitucionesque integran el sistema bancario, sirviendo también como	

Requerimiento técnico/ Funcional Gafi	Situación actual	Situación ideal	Ámbito legal Sudeban	Observaciones
lavado de activos y el financiamiento del terrorismo, deben aplicarse de una forma similar para propósitos ALA/CFT. Esto debe incluir la aplicación de una supervisión de grupo consolidada para propósitos ALA/CFT.			intermediariade confianza entre el sector financiero y las autoridades policiales y judiciales.	

Fuente: Entes reguladores gubernamentales (2012)

CAPÍTULO VI. Evaluación del nivel de brecha de los requerimientos de trazabilidad en el Sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Venezolana.

Para la evaluación de brecha es necesario tomar en cuenta no solo las entidades financieras, si no entidades gubernamentales encargadas de controlar los tributos (SENIAT), ya que nos pueden brindar información en cuento al nivel de riesgo de sus respectivas estructuras, clientes, productos, negocios, servicios, canales de distribución, mercados y jurisdicciones donde operan, con el fin de tomar las

medidas apropiadas, suficientes y eficaces, orientadas a identificar, evaluar y aplicar medidas para reducir la posibilidad de que en la realización de cualquier operación financiera sean utilizados como mecanismo para ocultar el origen, propósito y destino de los capitales ilícitos, o para desviar fondos de cualquier naturaleza hacia el financiamiento de grupos o actividades terroristas. Mitigando los riesgos que se derivan de la posibilidad que sean utilizados como mecanismos para legitimar capitales. En la figura 6 se puede observar como es la interacción con los entes gubernamentales, al realizar la colocación en el Sistema financiero.

Desde su inicio cuyo actor es el cliente, una vez que el banco recibe la transacción es evaluado por el área de legitimación de capitales, hasta llegar a entes externos como lo son el SENIAT y la ONA.

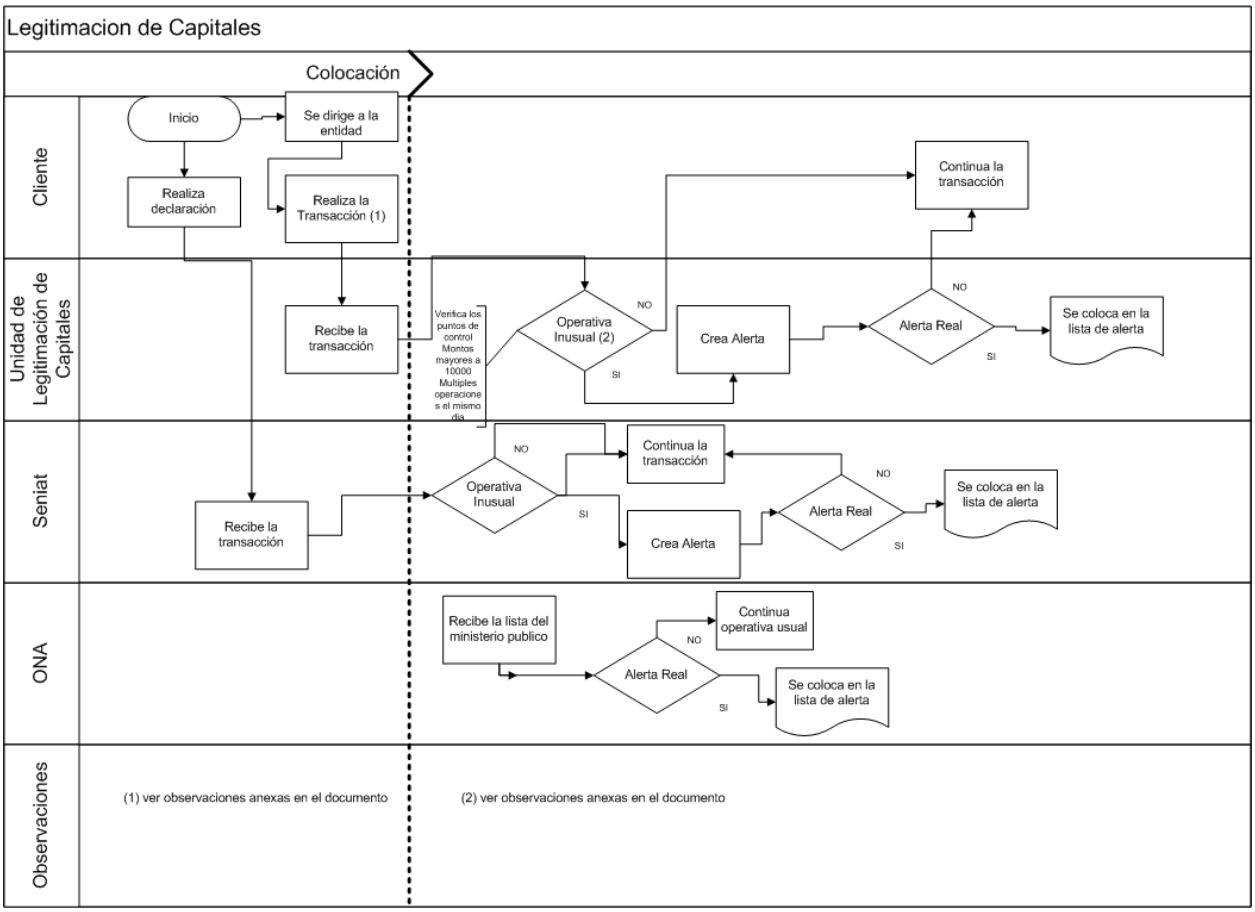

Figura 6. Legitimación de capitales y entes externos
Fuente: (caja venezolana de valores, 2017)

Por lo antes expuesto en la continua mejora del Sistema de Administración de Riesgo de Legitimación de Capitales, y el servicio hacia el cliente, interno y externo, se está en la búsqueda de una solución informática que le permita cumplir con las disposiciones legales y las normativas de SUDEBAN, y asimismo optimizar los procesos que se llevan en el país.

De acuerdo a la normativa emitida por la Superintendencia de Bancos y Otras Instituciones Financieras (SUDEBAN) Resolución N°: 119-10 de fecha 9 de marzo de 2010, los sujetos obligados, de acuerdo con la naturaleza y complejidad de sus negocios, productos y servicios financieros, al volumen de operaciones, a la región geográfica donde actúan, a la tecnología disponible y en concordancia con el nivel de sus riesgos de Legitimación de Capitales y Financiamiento al Terrorismo; deben formular, adoptar, implementar y desarrollar, un "Sistema Integral de Administración de Riesgos de Legitimación de Capitales y Financiamiento al Terrorismo" (SIAR LC/FT), que comprenda medidas apropiadas, suficientes y eficaces, orientadas a identificar, evaluar y aplicar medidas para reducir la posibilidad de que en la realización de cualquier operación financiera sean utilizados como mecanismo para ocultar el origen, propósito y destino de los capitales ilícitos, o para desviar fondos de cualquier naturaleza hacia el financiamiento de grupos o actividades terroristas.

TRAZABILIDAD

Se puede interpretar como la observación periódica y/o continua del comportamiento de un elemento dentro de un sistema, en este caso los elementos que nos ocupan son los distintos movimientos o transacciones que realiza un cliente; este monitoreo no tiene solo el objetivo conseguir información del estado actual de estos elementos, sino también recopilar información de estados anteriores del mismo, con el fin de suministrar datos suficientes para la activación de alertas. Hay que tomar en cuenta que la realización de rastros o trazas es una característica inherente de la existencia de los objetos en el proceso de legitimación y la habilidad de recopilarlos es lo que se define como trazabilidad, según la norma UNE 66901-

92 esta se define como “la capacidad de reconstruir el historial de la utilización o la localización de un artículo o producto mediante una identificación registrada”.

Cualquier tipo de sistema de trazabilidad comprende ciertos componentes básicos, los cuales interactúan entre sí para registrar, comunicar, almacenar, modificar y emitir informaciones específicas y relevantes a la entidad que estén sirviendo. Por esta razón es necesario que a través de la tecnología se pueda realizar las siguientes acciones registrar, modificar y gestionar la información cumpliendo los requisitos pertinentes.

Se requiere monitorear desde que un cliente realiza la transacción por medio de los diferentes canales del banco, hasta que la transacción es terminada, por ello es necesario tomar en cuenta desde que se inicia hasta el fin de la transacción, de igual manera es necesario guardar registro por cada módulo que va pasando la transacción (cliente, el canal, usuario ejecutor).

Módulos necesarios:

Módulo de análisis: Se debe tomar en cuenta que se requiere para el análisis de las transacciones módulos basados: reglas de scoring, arboles de decisión, Las listas OFAC, negras y PEPs.

Módulo de alertas y seguimiento: Donde se generan las alertas de prevención de Legitimación de Capitales y Financiamiento al Terrorismo, las cuales van a estar dirigidas a la Unidades de Legitimación, Banca Comercial, Banca Corporativa, Banca de Empresa, Banca Social y a la Banca Privada. De igual manera mediante el cual el usuario podrá analizar y responder las operaciones que se han incorporado al Sistema como "Operativa Sensible". El proceso de consulta y clasificación el cual consiste en asignar a un determinado movimiento o conjunto de movimientos un determinado estado (pendiente, normal, excepcionada o comunicada).

Módulo de administración: Para realizar todas las parametrizaciones dependiendo las leyes y normativas vigentes.

Módulo de comunicación: El proceso de comunicación de operativa sospechosa deberá permitir hacer llegar a la unidad de legitimación de capitales y a los responsables de Prevención de las Áreas y Unidades los datos, acerca de la operativa sospechosa detectada, realizar el seguimiento y estudio de los distintos comunicados generados, y dar la instrucción de generar expediente.

Módulo de generación de expediente: generación de un expediente que englobe los dichos datos asociados a la operativa sospechosa.

Módulo de perfiles y estadísticas: manejo de perfiles de acceso de los usuarios, los indicadores de clave de proceso, análisis estadísticos por clientes, por zona geográfica y por operativa.

Módulo de seguridad: gestión de usuarios, mecanismos de auditoría de la información, configuración de accesos, seguimiento de las operaciones realizadas en el sistema para garantizar el conocimiento de quién, cuando, qué se ha hecho y quién lo ha autorizado, por lo tanto debe permitir visualizar fecha, hora, IP, código de usuario, función ejecutada, y otros que se consideren necesarios, opciones de monitoreo de todas las operaciones, registro de logs.

Los sistemas de trazabilidad tienen importancia en términos de calidad, seguridad y prevención. La trazabilidad había sido definida previamente por los sistemas de gestión de calidad integral, y especialmente, por las normas ISO. En este sentido la ISO 9001:2008 la define como la habilidad para trazar la historia, aplicación o localización de lo que se esté considerando. Esta definición, quizás, no es tan clara como la que se daba en la norma ISO 8402:1994 en la que se definía como la

habilidad para trazar la historia, aplicación o localización de una entidad mediante la recopilación de datos.

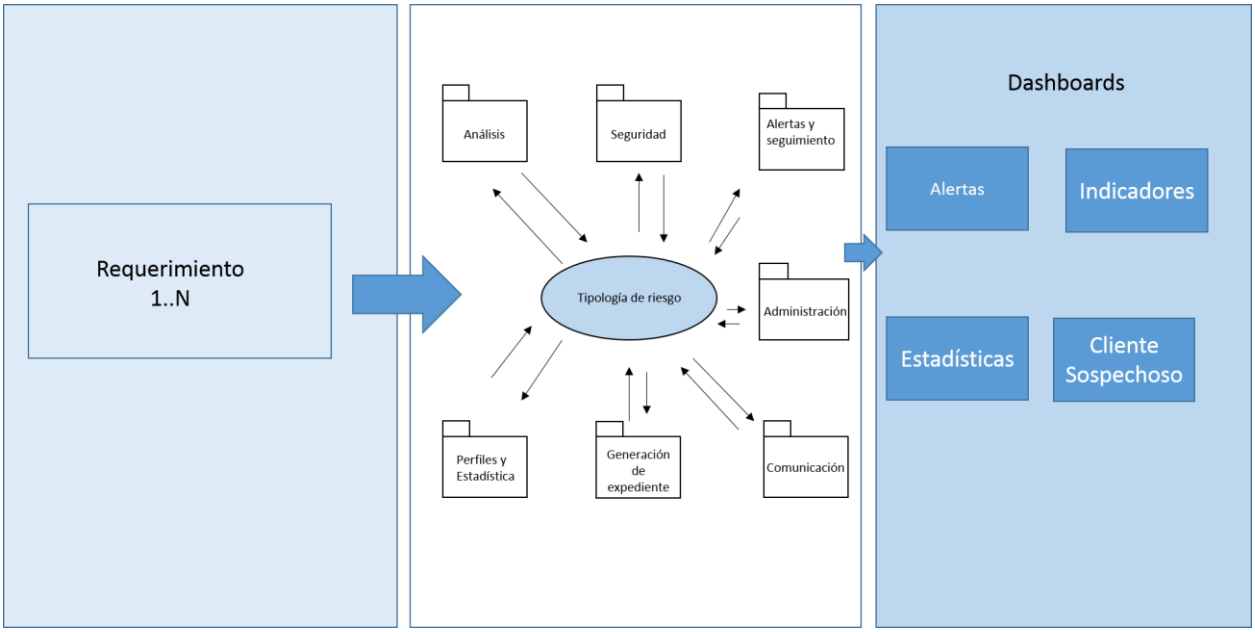

Figura 7. Tipología de riesgo.

Fuente: (Guevara, 2015)

El seguimiento de las transacciones de una persona puede aportar información suficiente para saber si la persona está legitimando capitales o financiando el terrorismo ya que existen múltiples factores que inciden para colocar a la persona como sospechosa. Como consecuencia, mientras más detallado el seguimiento y más precisa la información se podría detectar al sospechoso de forma más fácil y en tiempo real, y no solo observando el inicio de la transacción si no todo aquellos elementos que estuvieron involucrados.

Por tanto, la trazabilidad no solo es aplicable a los alimentos, sino que es algo más amplio que ha venido a constituir un gran apoyo, que debe formar parte en todas las etapas del desarrollo de un sistema, desde la captura de requerimientos hasta la implementación. Esto contribuirá al seguimiento de un requerimiento hacia adelante o hacia atrás, mostrando los efectos que puede tener ya sean la inclusión o exclusión de un nuevo requisito. También es de gran apoyo en la integración de nuevos módulos indicando las implicaciones que puedan tener en el sistema.

CAPÍTULO VII. Formular un modelo de evaluación integral del sistema de Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.

Según la tesis de Guevara (2015), define que los riesgos se dividen en tradicionales y específicos para este modelo se tomara en cuenta los riesgos específicos: que incluyen reputacional, legal, operacional, de contagio, transnacional y otros riesgos.

Figura 8. Clasificación de los riesgos

Fuente: (Guevara, 2015).

La banca pública maneja en su arquitectura modelo cliente – servidor, según Sommerville (1998) lo define como: un modelo de Sistema en el que dicho Sistema se organiza como un conjunto de servicios y servidores asociados, mas unos clientes que acceden y usan los servicios, el *core business* en estas entidades son muy parecidos, tienen algunas variaciones en la cantidad de servidores y aplicativos que manejan dependiendo de la magnitud de la cartera de clientes que cada entidad posee. Con entrevista en los grupo focales se presenta el *core business* general y se guardó el anonimato por razones de confidencialidad y seguridad.

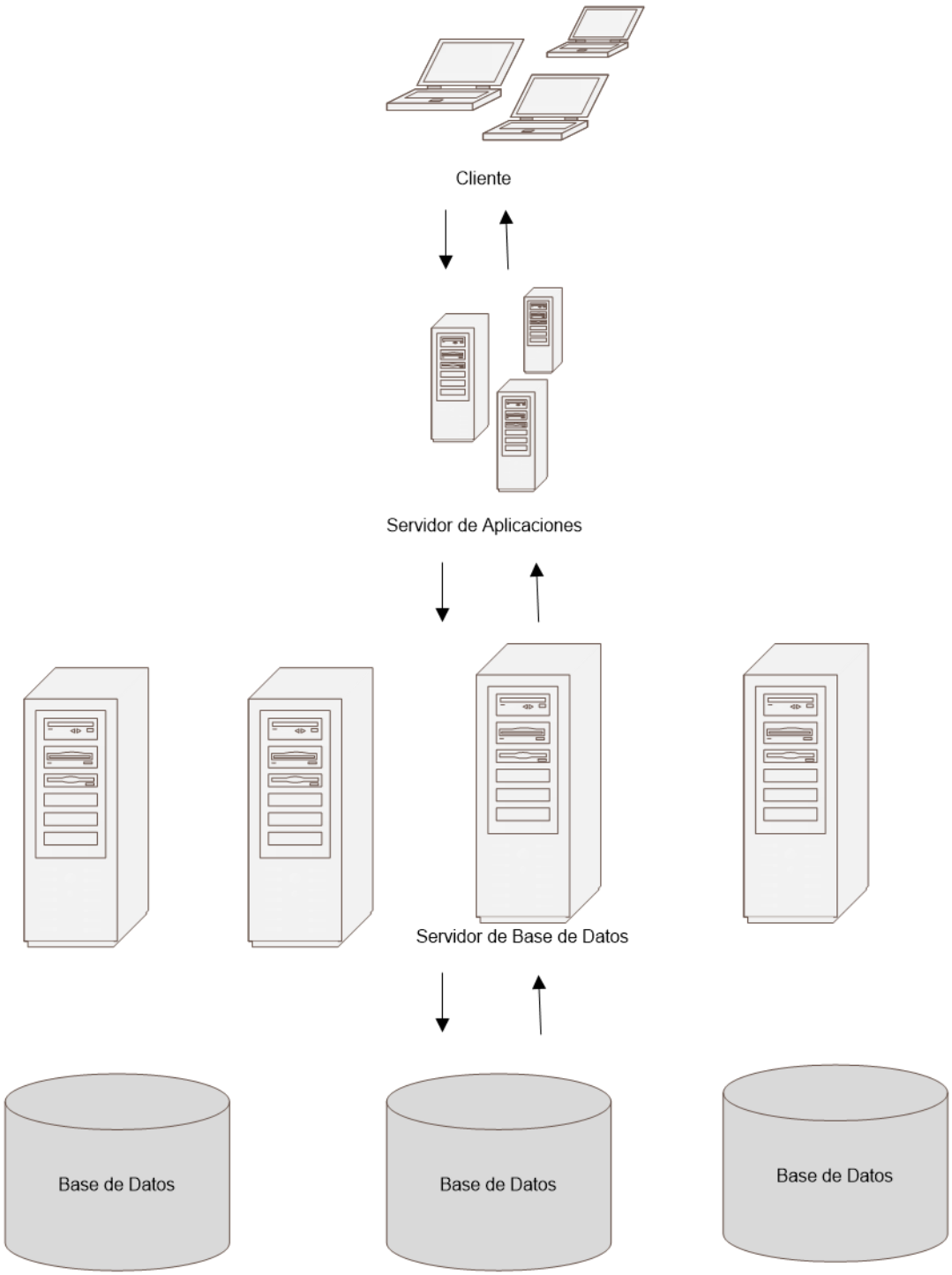

Figura 9. Cliente servidor Banca Pública Venezolana

Fuente: anónima

Según Guevara (2015) en su tesis indica que los Órganos y entes de control son órganos y entes de prevención, control, supervisión, fiscalización y vigilancia, de

conformidad con la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo y son los siguientes organismos (2012):

1.- La Superintendencia de las Instituciones del Sector Bancario.

2.- La Superintendencia de la Actividad Aseguradora.

3.- El Banco Central de Venezuela.

4.- La Superintendencia Nacional de Valores.

5.- El Ministerio del Poder Popular con competencia en materia de relaciones interiores y justicia, a través de sus órganos Competentes.

6.- El Servicio Nacional Integrado de Administración Aduanera y Tributaria.

7.- El Servicio Autónomo de Registros y Notarías.

8.- El Ministerio del Poder Popular con competencia en petróleo y minería, a través de sus órganos competentes

9.- El Ministerio del Poder Popular con competencia en materia de energía eléctrica.

10.- El Ministerio del Poder Popular con competencia en materia de planificación y finanzas, a través de sus órganos competentes.

11.-La Comisión Nacional de Casinos, Salas de Bingo y Máquinas Traganíqueles.

12.- El Ministerio del Poder Popular con competencia en materia de turismo.

13.- El Ministerio del Poder Popular con competencia en materia de ciencia y tecnología.

14.- El Ministerio del Poder Popular con competencia en materia de industrias.

15.- El Ministerio del Poder Popular con competencia en materia de comercio.

16.-El Consejo Nacional Electoral.

17.- Cualquier otro que sea designado mediante ley o decreto.

Estos entes son importantes ya que son primordiales como fuente de información para el expediente del cliente.

La inteligencia de negocio BI según Gartner, es un proceso interactivo para explorar y analizar información estructurada sobre un área (normalmente almacenada en un *datawarehouse*), para descubrir tendencias o patrones, a partir de los cuales derivar ideas y extraer conclusiones.

El proceso Business Intelligence incluye la comunicación de los descubrimientos y efectuar los cambios.

Según el Data Warehouse Institute define inteligencia de negocio como la combinación de tecnología, herramientas y procesos que permiten transformar datos almacenados en información, esta información en conocimiento y este conocimiento dirigido a una estrategia.

Para el modelo es necesario emplear inteligencia de negocio, ya que ofrece múltiples ventajas en cuanto a gestión de clientes, productos y manejo de transacciones, permitiendo así el cruce de los distintos datos, brindando mejores tiempos de respuesta.

Para una entidad financiera pequeña se presentaría una arquitectura de la siguiente manera:

Observando la figura 10, de arriba abajo se puede ver una base de datos que contiene información refente a clientes, transacciones, productos, analistas, tipos de alarma, listas negras, listas ONA, luego se procede a la extracción, procesamiento y carga de datos, se almacena en una base de datos, para luego ser mostrado en el dashboards, utilizando herramientas de BI, dando como resultado al usuario de legitimación de capitales reporte alarmas, lista de alertas (por cliente, por tipología, por zona geográfica), entre otros.

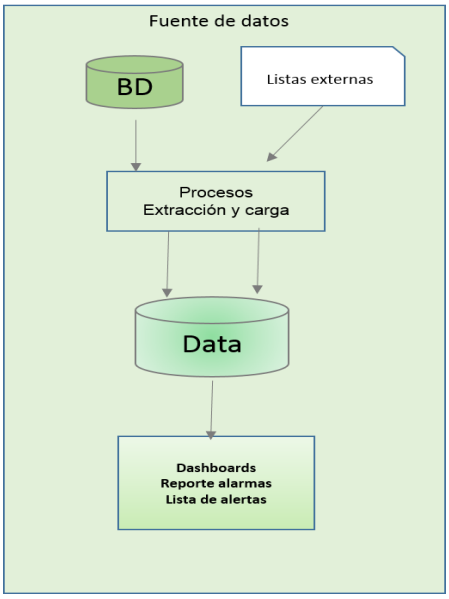

Figura 10. Arquitectura banco pequeño para legitimación de capitales.

Fuente: (msdn Microsoft, 2012)

Para el modelo de evaluación integral del sistema de información administración de riesgo de legitimación de capitales en la banca pública venezolana. Se presenta en la figura 11 una arquitectura general de la siguiente manera.

En la figura 11, se muestra en el recuadro A de izquierda a derecha las distintas fuentes de datos: base de datos Sql Server, base de datos Oracle, base de datos mainframe, listas externas (OFAC, DEA, Comunidad Europea, PEPs, entes gubernamentales, entre otras), obteniendo de ellas un resultado para realizar la revisión de los clientes que aparezcan en la lista previamente mencionadas, muestra el proceso de extracción para localizar y extraer datos, de manera tal que cause el menor impacto en el origen ya que vienen de distintas base de datos como se menciona anteriormente, procesamiento / transformación es parte de la homologación de datos para su futuro uso y carga de los datos, el segundo cuadro identificado con la letra B muestra el almacenamiento de datos, en el extremo superior es la minería de datos provenientes de las distintos bancos que conforman la banca pública venezolana (Banco de Venezuela, Banco del Tesoro y Banco Bicentenario), suministrando información relevante para el modelo y alimentando el *datawarehouse,* facilitando la aplicación de técnicas estadísticas y de análisis para

encontrar las relaciones implícitas entre los datos que se tienen, y mejorando tiempos de respuesta y fiabilidad en la información, ya que mientras menos manipulación manual de data, la cantidad de errores disminuye. Y como resultado final en el recuadro C se tiene la explotación de la información a través de las herramientas de inteligencia de negocio, que se pueden observar como la consulta general, a través del *dashboards* con toda la información requerida de acuerdo al tipo y necesidad del usuario tanto de la unidad de legitimación, como a las distintas agencias, puede mostrar los clientes sospechosos, movimientos y *scoring*, comportamiento habitual, evaluación del *scoring*, variación, minería de datos, indicadores, zonas geográficas, reportes y estadísticas, entre otros.

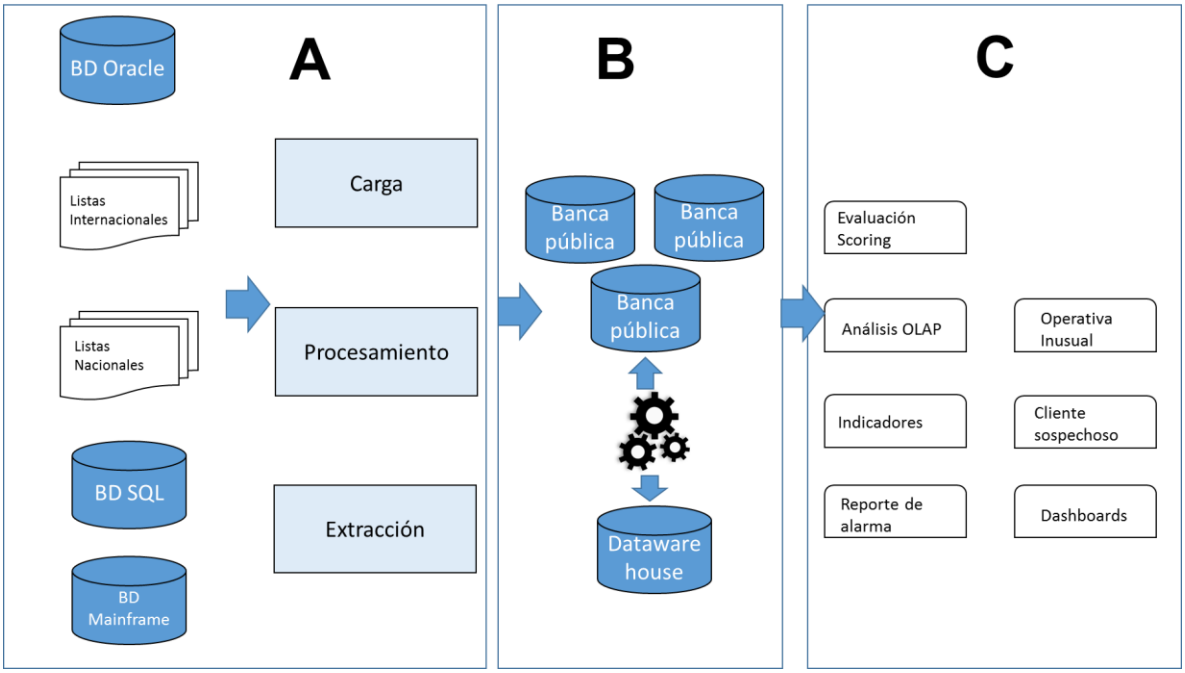

Figura 11. Arquitectura general para el modelo de evaluación integral del sistema de información administración de riesgo de legitimación de capitales en la banca pública venezolana.

En función de la necesidad de la banca en materia de validación de los archivos llamados átomos, se debe contar con un sistema cuyas áreas de trabajo se encuentren las validaciones de los datos contenidos en los átomos basado en las reglas establecidas por la SUDEBAN. Esta solución debe contemplar un repositorio

en el cual se almacenen los datos originados por el banco, y en otro un repositorio con los reportes de la validación de los datos por cada átomo.

En este debe existir también un conjunto de procesos que se encarguen de extraer los datos de origen, y los transformen en reportes de validación a fin de que encajen con el formato definido por la SUDEBAN para cada átomo, con la finalidad que la banca transmita los átomos basado en las reglas establecidas por el ente regulador.

Se muestra en la figura 12, la representación del problema de manera gráfica a través del diagrama de entidad relación que se muestra a continuación, donde las entidades son: cliente, revisiones, analistas, alertas y situación. En este se identifica la interrelación entre las diferentes entidades.

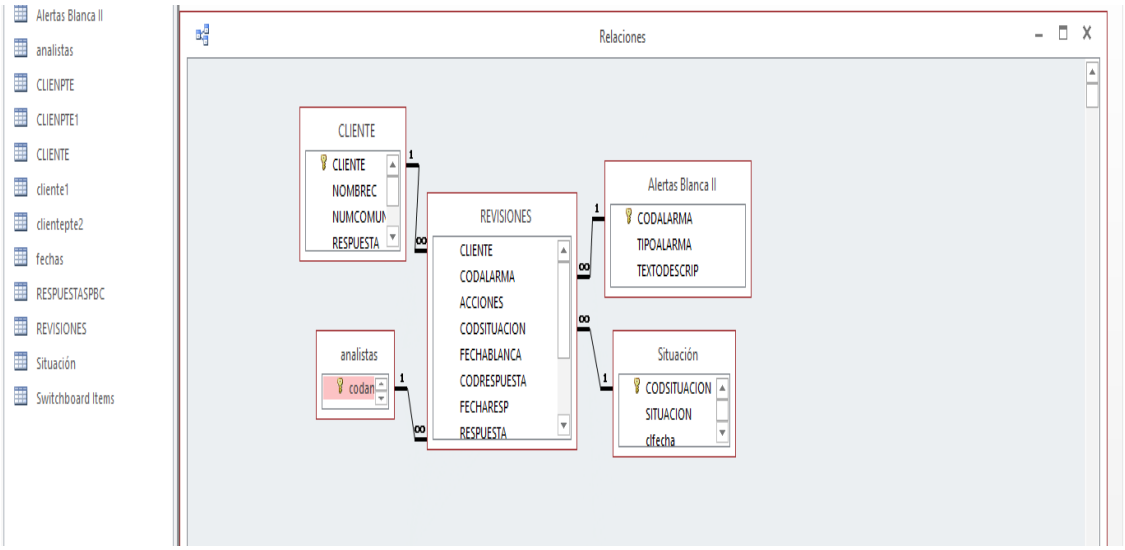

Figura 12. Entidad relación para el modelo propuesto.

Fuente: Propia de la investigación.

A continuación se muestra en la figura 13, el Core de un banco perteneciente a la banca pública, se puede observar que los Core de los bancos están de una forma u otra estandarizados, varían los aplicativos que cada uno posee por lo tanto el modelo es factible aplicarlo a la banca pública.

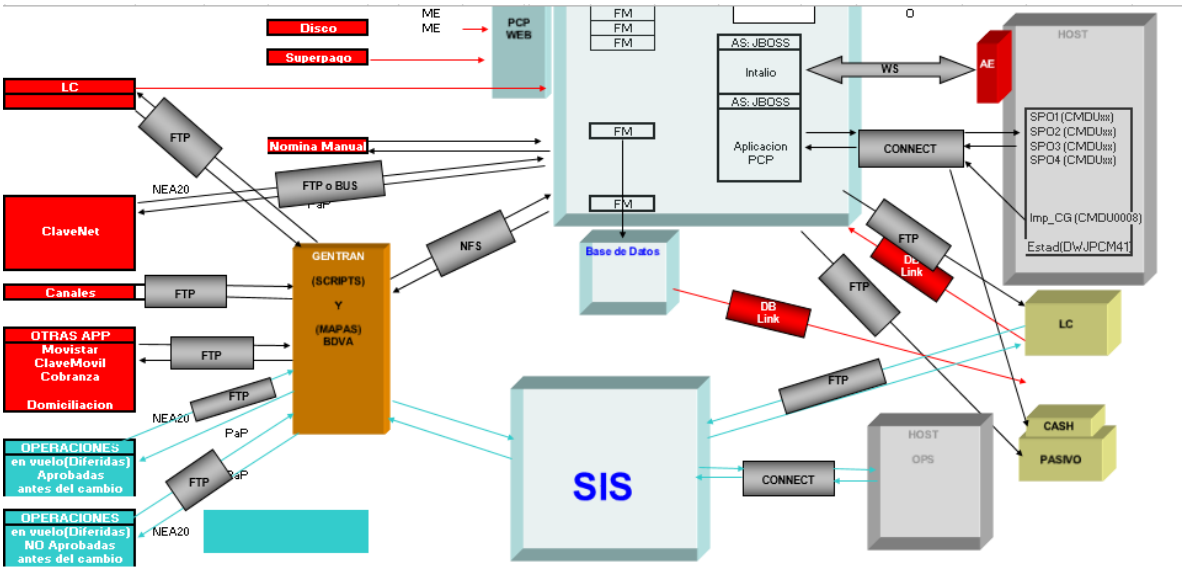

Figura 13. Core banca pública.

Fuente: (Rivero, 2016)

Basado en toda la información suministrada en el transcurso de la investigación se propone el siguiente dashboard:

Se utilizó como herramienta de trabajo solo con fines educativos Sisense.

En la figura 14 se muestra el dashboard correspondiente a las alarmas, estas alarmas permiten a la unidad de prevención y control de legitimación de capitales y financiamiento al terrorismo, concentrar su atención en los clientes que han tenido un comportamiento inusual en su operativa bancaria:

Figura 14. Prototipo dashboard alarmas

Fuente: Propia de la investigación.

Alarma en función del *scoring* y los movimientos realizados, alarma de nivel 1 muestra los *n* primeros *scoring*.

Alarma en función del comportamiento habitual.

Alarma en función de la evolución del *scoring* si potencialmente varía el comportamiento normal del cliente.

Alarma en función de la evolución en el tiempo de las pautas de comportamiento habituales.

Alarma en función de la evolución en el tiempo de las pautas de comportamiento habituales.

En la figura 15 se muestra las distintas categorias de alarmas y los clientes involucrados.

Figura 15. Prototipo Dashboards alarmas por cliente.

Fuente: Propia de la investigación.

En la figura 16 se muestra el porcentaje de las alarmas reales, entiéndase como aquellas alarmas que desde el inicio se presentaron y fueron comprobadas, y los falsos positivos aquellos que un inicio se colocaron como alarmas pero al revisar el caso, resulto que la alarma no procedía.

Figura 16. Prototipo Dashboards alarmas.

Fuente: Propia de la investigación.

En la figura 17 se muestra que zonas del país son más vulnerable a la legitimación de capitales y la cantidad de alarmas presentadas por ciudades.

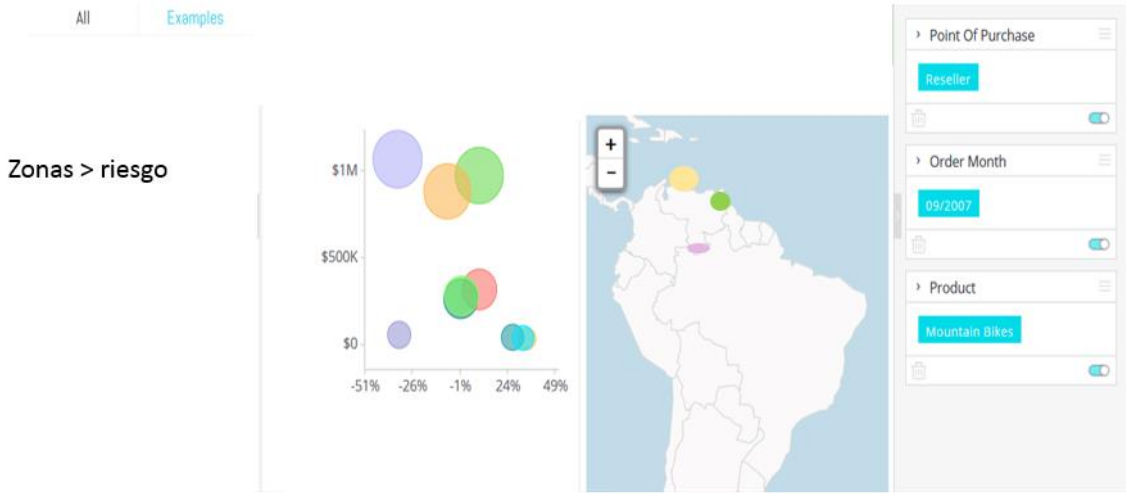

Figura 17. Prototipo Dashboards zonas riesgo.

Fuente: Propia de la investigación.

Para la elaboración técnica del modelo se presentan a continuación compañías reconocidas y se describe su beneficio:

Tabla 9. Empresas de Software

Empresa	Beneficios
IBM (1)	Las **soluciones de inteligencia de negocio de IBM** incluyen prestaciones de autoservicio para proporcionar agilidad al negocio con un método de plataforma empresarial, disponible en local o en el *cloud*, que permite a los clientes acelerar el crecimiento y el éxito. Un rango de funcionalidades analíticas diseñadas para integrarse entre ellas y con soluciones de terceros, con la finalidad de cubrir sus necesidades de inteligencia de negocio, con la certeza y seguridad de que podrá ampliar la solución con el paso del tiempo para cumplir futuros requisitos
ORACLE (2)	Oracle Business Intelligence (BI) es una cartera de tecnología y aplicaciones que proporciona el primer sistema integral de gestión del rendimiento empresarial integrado de la industria, incluida la base y las herramientas de BI: conjunto integrado de consultas, informes, análisis, alertas, análisis móviles, integración y administración de datos e integración de escritorio, así como aplicaciones de gestión del rendimiento financiero líderes en su categoría, aplicaciones de BI operacionales y almacenamiento de datos.

SAP (3)	Poderoso software de BI le permite poner información lista para tomar decisiones dentro del alcance de los usuarios comerciales. Con nuestra plataforma de análisis, puede aumentar la capacidad de respuesta, reducir los costos de TI y la carga de trabajo, y lograr una mejor toma de decisiones en toda su organización. Obtenga inteligencia empresarial en tiempo real a partir de cualquier información Aumentar la autonomía del usuario al exponer los datos en términos comerciales simples Haga que el consumo de información sea simple, personalizado y dinámico Benefíciese de una infraestructura de información flexible y escalable
HP (4)	Los Servicios de Modernización de Business Intelligence, diseñados para ayudar a los clientes a comprender, gestionar y aprovechar los datos dentro de su empresa y así mejorar la participación del cliente, ayudando a crear nuevas oportunidades de negocio y reducir los gastos.

Fuente: (1) https://www.ibm.com/ibm/ve/es/?lnk=vehpv18l2

(2) https://www.oracle.com/ve/solutions/business-analytics/business-intelligence/index.html

(3) https://www.sap.com/latinamerica/index.html

(4)http://www.hp.com/hpinfo/newsroom/press_kits

/2009/lasvegasevents2009/fs_BIS.pdf

Capitulo VIII. Aplicar una prueba de concepto del modelo de evaluación integral del sistema Información Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.

Según slmsc (2017) el objetivo de la prueba de concepto es valorar el concepto de producto antes de comenzar su desarrollo técnico. El concepto es la idea de producto desarrollada en detalle. Es necesario para una prueba de concepto que explotemos algunos casos de usos, en el proyecto existen muchos casos de usos, para efecto de la prueba se tomara en cuenta los siguientes casos:

Caso 1:

El cliente genera alerta debido a una operación que para las reglas del negocio está clasificada como operación sospechosa, puede entrar a las diferentes alarmas:

Alarma 1: Alarma en función del *scoring* y los movimientos realizados, alarma de nivel 1 muestra los *n* primeros *scoring*.

Alarma 2: Alarma en función del comportamiento habitual.

Alarma 3: Alarma en función de la evolución del *scoring* si potencialmente varía el comportamiento normal del cliente.

Alarma 4: Alarma en función de la evolución en el tiempo de las pautas de comportamiento habituales.

Alarma 5: Alarma en función de la evolución en el tiempo de las pautas de comportamiento habituales.

El cliente tiene operaciones en las que su monto fraccionado no supera cierto umbral, pero que sumadas (acumuladas) son mayores a un importe mínimo acumulado (activa la alarma 5). Por lo tanto pasa a la lista de persona sospechosa, se valida y verifica la información, se le genera expediente, y es reportado ante los entes de seguridad.

O es un falso positivo y pasa a las estadísticas, quitándole la marca de cliente sospechoso y se coloca la excepción.

Utiliza para realizar esta prueba los siguientes módulos: Análisis: para la revisión de las transacciones y colocarlo en alerta. Alertas y seguimiento: genera la alertas de prevención de Legitimación de Capitales y Financiamiento al Terrorismo, las cuales van a estar dirigidas a la Unidades de Legitimación y Banca Comercial ya que es un cliente natural. De igual manera se realizara la clasificación del movimiento a un determinado estado (pendiente o comunicada). Comunicación: Comunica la operativa sospechosa hace llegar a la unidad de legitimación de capitales y a los responsables de Prevención de las Áreas y Unidades, los datos acerca de la operativa sospechosa detectada, permite realizar el seguimiento y estudio de los distintos comunicados generados, y dar la instrucción de generar expediente. Generación de expediente: generación de un expediente que contiene datos asociados a la operativa sospechosa. Perfiles y estadísticas: Se maneja perfiles de acceso de los usuarios, y los diferentes indicadores claves del proceso, análisis estadísticos por clientes con alarma 5. Ver figura 18.

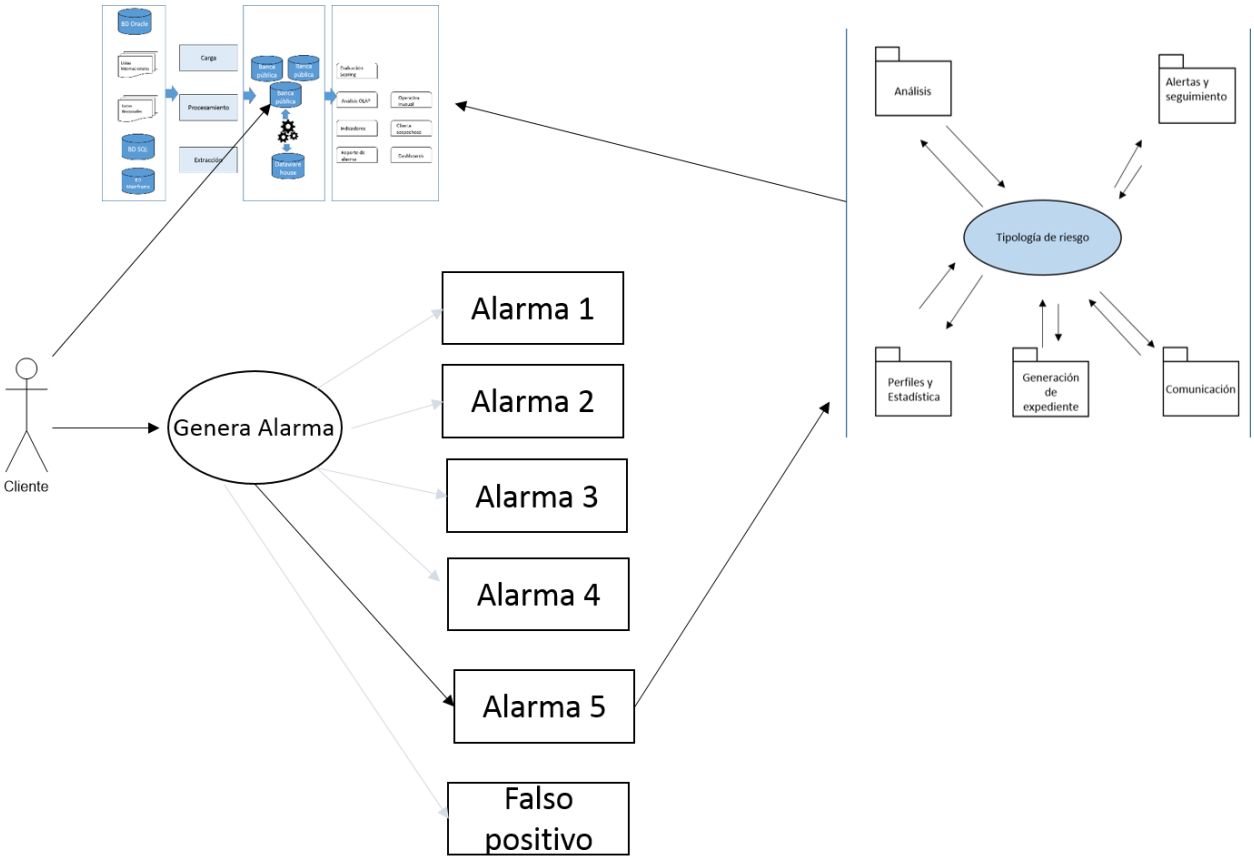

Figura 18. Caso generar alerta 5

Caso 2:

Un ente gubernamental solicita una nueva parametrización dependiendo la zona geográfica del cliente y requieren agregar nueva lista de ente externo.

Se parametriza a través de la aplicación, se incorpora la nueva lista a la fuente de datos, y continua operativa habitual, tomando en cuenta el nuevo requerimiento asignado.

Como lo muestra en la figura a continuación utiliza los módulos: administración: Para realizar todas las parametrizaciones solicitadas por los entes gubernamentales, y análisis: Por la inclusión de una nueva lista externa.

Y en la figura 19 perteneciente al modelo de inteligencia de negocio se muestra que se debe agregar la nueva lista a la fuente de datos, del modelo de evaluación integral del sistema Información Administración de Riesgo de Legitimación de Capitales en la Banca Pública Venezolana.

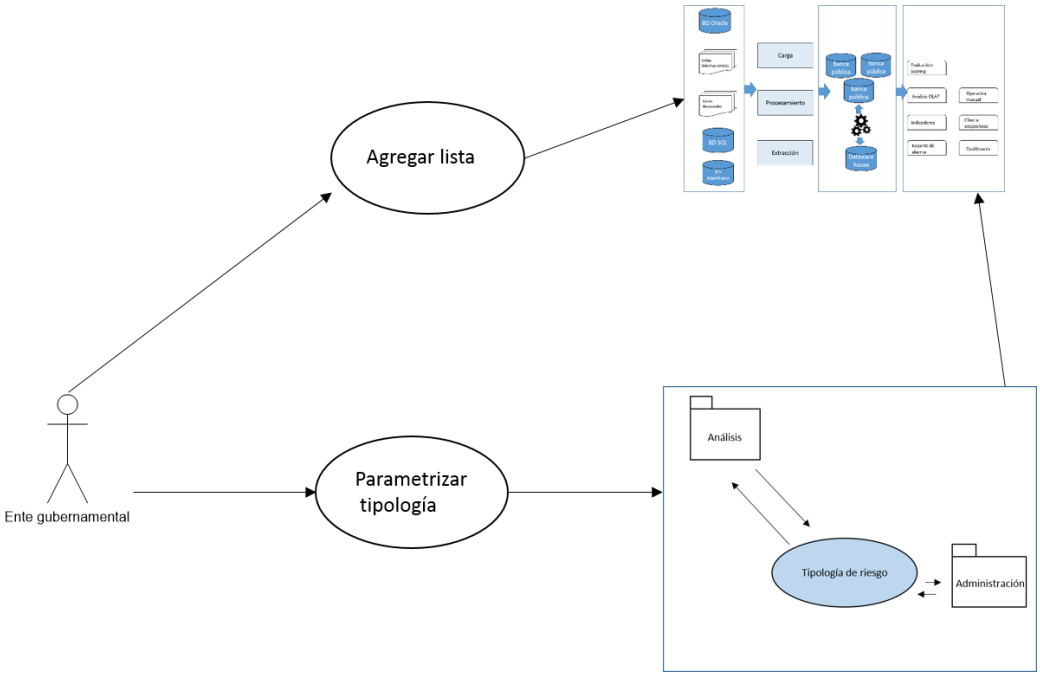

Figura 19. Caso solicito ente gubernamental

Caso 3: Ocurre un ataque informático al aplicativo, logran utilizar cuenta para legitimar capitales, se enciende alarma de operativa inusual, se valida con el cliente

el cual indica que no realizo la operación, se procede activar protocolo de seguridad, y el auditor se encarga de revisar a través del módulo de seguridad, la trazabilidad de las operaciones realizadas en el sistema para garantizar el conocimiento de quién, cuando, qué se ha hecho y quién lo ha autorizado en todo momento, por lo tanto debe permitir visualizar fecha, hora, IP, código de usuario, función ejecutada, y otros que se consideren necesarios.

En este caso se emplearon los módulos: Seguridad: para la gestión de los mecanismos de auditoría de la información, seguimiento de las operaciones realizadas en el sistema, verificación de logs. Alertas y seguimiento: Se generan alertas de prevención de Legitimación de Capitales y Financiamiento al Terrorismo, el usuario analiza y responder las operaciones que se han incorporado al Sistema como "Operativa Sensible". Ver figura 20

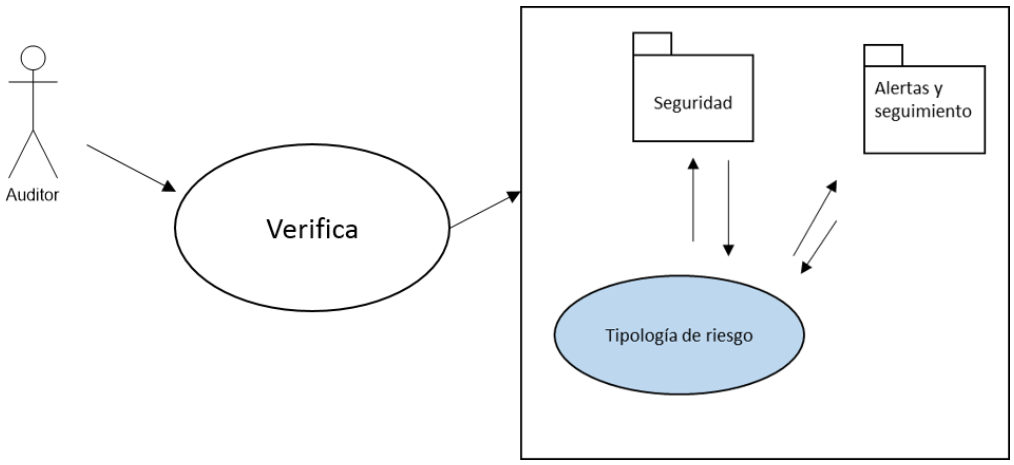

Figura 20. Caso de auditoria

Estos resultados cumplen a nivel conceptual ya que sirven para todos los casos estipulados por Basilea desde el proceso de estandarización de datos hasta los módulos para la determinación de riesgos, de igual manera cumple para la norma ISO 27001, proporcionando certeza con respecto a la seguridad de información, trazabilidad, usabilidad y escalabilidad.

CAPÍTULO IX. CONCLUSIONES Y RECOMENDACIONES.

La identificación de los requerimientos permitió esquematizar a través de un marco lógico de forma detallada los requisitos exigidos por las normas y leyes vigentes, y agregar lo solicitado por el GAFI. Esta identificación es de suma importancia ya que muchos problemas que se presenta en la ingeniería de software vienen dados por la falta de precisión al momento de identificar los requerimientos.

Para la evaluación de brecha en este objetivo, fue necesario abstraerse del marco de la banca pública y agregar organismos del estado que sirven de control, además forman parte importante en el manejo de información del cliente, de igual forma se realizó la trazabilidad, con el fin de observar los componentes básicos y la acciones principales, y se llegó a la conclusión que mientras más detallada y precisa la información, mejor serán los resultados, ya que fue analizado cada punto de la situación actual y de lo solicitado, obteniendo el grado de cumplimiento y lo que falto contemplar para nivelarse con entidades bancarias internacionales. De igual forma se observó que se puede involucrar a entes reguladores, obteniendo mejor precisión en cuanto a la información y la trazabilidad de cada cliente.

En líneas generales la banca pública maneja un standard en el core business en su organización, lo cual permitió formular un modelo con una arquitectura general, basado en inteligencia de negocio donde se incluye cada uno de los bancos de la banca pública, y la interrelación de la data con el fin de mejorar el desempeño en cuanto a control de legitimación de capitales y financiamiento al terrorismo. Aportando así grandes ideas para extrapolar este modelo integrado no solo a la banca pública si no a la banca privada.

Se realizó la prueba de concepto con el fin de validar el modelo planteado, observándose una manifestación sustancial al aplicar los casos que ocurren en la operativa diaria. Por tal motivo a través de la prueba de concepto se observó que el modelo es ciertamente posible y sería de gran utilidad implantarlo. Ya que cumple con lo expuesto en Basilea dando gran valor al cumplimiento de sus normativas sin olvidar la seguridad de la información.

El estudio detallado de la investigación permitió la revisión de las fuentes teóricas y marco regulatorio, tanto nacional como internacional permitiendo modelar los

controles financieros a través de la automatización e interrelación de datos para la prevención de la legitimación de capitales y financiamiento al terrorismo.

Permitiéndose así proporcionar información confiable y veraz con relación a las acciones realizadas por el cliente, aportando gran avance en el proceso de legitimación y riesgos presentes en la operativa, fortaleciendo el desarrollo de la finanzas en el sistema económico de Venezuela, aportando credibilidad, ya que con este modelo se mejoraría los desactualizados controles administrativos en cuanto a rastreo de operaciones y control de legitimación se trata.

Recomendaciones

De la información obtenida, en la presente investigación se presenta una serie de recomendaciones aplicables en la materia estudiada. En este sentido, bajo la premisa de que las técnicas de prevención también deben evolucionar para contrarrestar los nuevos tipos de ataques de la legitimación de capitales, a continuación se presentan las recomendaciones para enfrentar la legitimación de capitales en el sistema financiero venezolano entre las que se mencionan:

Formar un grupo Egmont venezolano, donde participen las entidades bancarias venezolanas y entes gubernamentales con el fin de innovar y refinar el tema de legitimación de capitales en Venezuela, y ser guía de buenas prácticas para el mundo.

Revisar cada banco con el fin de adaptarse a los requerimientos de la institución sin perder los lineamientos exigidos por los entes regulatorios.

Hacer revisiones periódicas tanto de la plataforma, como del personal que labora en la institución con el fin de evitar situaciones que pongan en riesgo la operativa diaria.

Realizar y documentar auditorias con el fin de verificar el buen desempeño y el cumplimiento de las leyes.

Tomar como ejemplos bancos internacionales y aplicar las mejores prácticas siempre y cuando no interfiera en las leyes del país.

Como próximo paso, llevar el modelo conceptual a la práctica, aplicando conjuntamente las normas *ISO/IEC 27001.*

Los aspectos a investigar: Seguridad y governance de la tecnología información, seguridad de información administrada, modelos integrados de sistemas de información, big data manejo de grandes volúmenes de información.

REFERENCIAS BIBLIOGRÁFICAS

Alfonso, I. (1999). Técnicas de investigación bibliográfica (8va ed.).Caracas: Contexto.

Altuve S y Rivas A. (1998). Metodología de la Investigación. Módulo Instruccional III. Caracas: Universidad Experimental Simón Rodríguez.

Arias, F. (2012). Proyecto de investigación: Introducción a la metodología, científica. 6ta edición. Editorial Episteme. Caracas. Venezuela.

Asamblea Nacional de la República Bolivariana de Venezuela (2009). Ley General de Bancos y otras Instituciones Financieras. Gaceta Oficial No. 5.947 Extraordinario, de fecha 23 de diciembre de 2009. Venezuela.

Bavaresco, A. (1996). Proceso Metodológico de la Investigación. 3era. Edición. Maracaibo: Servicios Bibliotecarios de la Universidad del Zulia.

Bello, G. (2009).Operaciones Bancarias en Venezuela: teoría y práctica. Venezuela. Universidad Católica Andrés Bello.

Bitam. (2011). Business Intelligence. Recuperado el 15 de diciembre de 2011, de Bitam:http://www.bitam.com/bitamwebesp/solutions_business_intelligence.php

Berkowitz, J., y O'Brien, J. (2002). How accurate are Value-at-Risk models at commercial banks, Journal of Finance 58, 1093-1111.

Bonczek, R., Holsapple, C., y Whinston, A. (1981). Foundations of Decision Support Systems, New York: Academic Press, 19, 19 - 20.

Bzaltynova, Z., y Williams, J. (2013). Developments in business intelligence software. Journal Of Intelligence Studies In Business, 3, 40-54.

Caja Venezolana de Valores. (2017). Recuperado el 05 de noviembre de 2017 de: https://www.cajavenezolana.com/cvv/indexs.asp

Carey, M. (1998). Credit risk in private debt portfolios, Journal of Finance 53, 1363-1387.

Catarineu-Rabell, E., Jackson, P., y Tsomocos, D. (2002). Procyclicality and the newBasel accord – banks' choice of loan rating system, Working paper, Bank of England.

Código de Ética del Colegio de Ingenieros de Venezuela – 1996.

Comité de Supervisión Bancaria Basilea II. (2006). Retos cuantitativos. Documento en línea. Recuperado el 20 de Junio de 2011 de redeconomia: http://www.redeconomia.org.ve/documentos/informa3/retobasileaII.pdf.

D'Antoni, J., y Lopez, K. (2014). The Modern Data Warehouse--How Big Data Impacts Analytics Architecture. Business Intelligence Journal. 2014, Vol. 19 Issue 3, p8-15. 8p.

Dey, S., y Gadda, K. (2014). Business intelligence for public sector banks in india: a case study- design, development and deployment. Journal Of Finance, Accounting & Management, 5(2), 37-58.

Espiñeira, Sheldon y Asociados (2008). Gestión Integral de Riesgos: Fundamentos y Tendencias. Venezuela. Universidad Católica Andrés Bello.

Fabian, E. (1998). El delito de Blanqueo de Capitales. Madrid.

FATF. (2010), Best Practices Confiscation (Recommendations 3 and 38), FATF, Paris, France. Recuperado el 25 de Mayo de 2011, de FATF en: www.fatfgafi.org/topics/fatfrecommendations/documents/bestpracticesconfiscationrecommendations3and38.html

FATF. (2012). Operational Issues Financial Investigations Guidance, FATF. Recuperado el 11 de Diciembre de 2013, de fatf en: www.fatfgafi.org/topics/fatfrecommendations/documents/operational_issues_financial.pdf.

Fontnouvelle, P., DeJesus V., Jordan, J., y Rosengren, E. (2003). Using Loss Data to Quantify Operational Risk. Federal Reserve. Bank of Boston.

Hendricks, D. (1996). Evaluation of Value-at-Risk models using historical data, Economic Policy Review. Federal Reserve Bank of New York, 39-46.

GAFI. (2012). Operational Issues Financial Investigations Guidance, FATF. Recuperado el 11 de Diciembre de 2013, de fatf en: www.fatfgafi.org/topics/fatfrecommendations/documents/operational_issues_financial.pdf.

Guevara, L. (2015).La Legitimación de Capitales en el Sistema Financiero Venezolano. (Trabajo Especial de Grado). Recuperada Universidad de Carabobo.

Hernández Sampieri R, Fernández Collado C, Baptista Lucio P. 2003. Metodología de la Investigación. 3ª Edición. Mc Graw-Hill Interamericana; México DF, México

Horst, E. (2006). Las juntas directivas y el manejo del RIESGO. Debates IESA, 11, 42-45.

Información Tecnológica. (2005). Recuperado el 5 de Diciembre de 2013, de scielo.cl: http://www.scielo.cl/scielo.html

Kumar , V. (2013). Data analysis using business intelligence tool. Faculty of San Diego State University. Spring.

Laudon, K. y Guercio, C. (2009), E-commerce: Negocios, Tecnología y Sociedad, Pearson, pp.10, 19, 302, 524.

Luciani, J. (2006). La triple vertiente del riesgo de legitimación de capitales. Ámbito Jurídico, 1, 1.

Mackie-Mason, J. y White, H. (1996).Evaluating and selecting digital payment mechanisms. Laurence Erlbaum.

Martínez, M., y Coronado, G. (2003). Indicadores para la evaluación integral de la productividad académica en la educación superior. Revista ELectrónica de Investigación y Evaluación Educativa, v. 9, n. 1. Recuperado el 7 de Enero de 2012, en uv: http://www.uv.es/RELIEVE/v9n1/RELIEVEv9n1_2.htm.

Mejía, G. (2008). Fundamentación de un sistema de evaluación a la Gestión Integral de los Procesos Universitarios, sobre la Base de la Auditoría como Proceso, para la

Universidad Católica de Oriente. Revista Ciencias Estratégicas, Vol 16, Núm. 19, enero-junio, 2008, pp. 33-45

Mohammed, M. (2010). Phishing website detection using intelligent data mining techniques. University of Bradford.

Pons, P. (2010). Comentarios al Proyecto de Ley de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo: Nuevas Obligaciones para Entidades Financieras y otros Sujetos Obligados. Actualidad Jurídica (1578-956X), (25), 61-73.

Ramírez, P. (2006). Estudio y Propuesta para Implantar una Unidad De Inteligencia Financiera en Venezuela. (Trabajo Especial de Grado). Recuperada Universidad Nueva Esparta.

Resolución Nro. 119-10, Superintendencia de Bancos y Otras Instituciones Financieras (2010, marzo 9). Gaceta Oficial de la República Bolivariana de Venezuela, 37.328, Noviembre 20, 2001.

Resumen banca publica. 2017. Recuperado el 11 de noviembre de 2017, disponible en: https://es.scribd.com/doc/70139555/RESUMEN-BANCA-PUBLICA-2

Sabino, C. (2007). El proceso de investigación. Caracas: Panapo.

Sans, J. y Rahnema, A. (2004). Basilea II. Una nueva forma de relación banca – Empresa. España. Editorial McGraw Hill Interamericana

Superintendencia de Bancos y otras Instituciones Financieras (SUDEBAN) (2006). Riesgos operativos. Documentos en línea. Recuperado el 22 de Junio de 2011, disponible en: http://www.sudeban.gob.ve/webgui/.

Superintendencia de Bancos y otras Instituciones Financieras (SUDEBAN) (2009). Boletín Informativo. Anexos estadísticos. Memoria Anual 2009. Documento en línea. Recuperado el 03 de Julio de 2011, Disponible en: http://www/sudeban.gob.ve/webgui/.

Turban, E., McClean, E., y Wetherbe, J. (2001). Tecnologías de información para la administración. México: CESSA. 970.

UPEL. (2005). Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales. Caracas: FEDUPEL.

Yáber, G. y Valarino, E. (2003). Tipología, fases y modelo de gestión para la investigación de postgrado en Gerencia. Venezuela.

Zopp. (2014). Recuperado el 3 de Noviembre de 2017, de http://www.pmsj.org.pe/nweb/publicas/CLAD/Metodologia_ZOPP_GTZ.pdf