

# Análisis de las aplicaciones informáticas de control interno en entidades bancarias para la detección y prevención de lavado de dinero.

Elsa Beatriz Suarez Kimura y Diego Sebastian Escobar.

Cita:

Elsa Beatriz Suarez Kimura y Diego Sebastian Escobar (2010). *Análisis de las aplicaciones informáticas de control interno en entidades bancarias para la detección y prevención de lavado de dinero. XII Jornadas de Investigación y Reflexión de Temas Contables en las Cátedras. Departamento Pedagógico de Contabilidad, Facultad de Ciencias Económicas, Universidad de Buenos Aires*.

Dirección estable: <https://www.aacademica.org/escobards/54>

ARK: <https://n2t.net/ark:/13683/ptuD/t4M>



Esta obra está bajo una licencia de Creative Commons.  
Para ver una copia de esta licencia, visite  
<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es>.

Acta Académica es un proyecto académico sin fines de lucro enmarcado en la iniciativa de acceso abierto. Acta Académica fue creado para facilitar a investigadores de todo el mundo el compartir su producción académica. Para crear un perfil gratuitamente o acceder a otros trabajos visite:  
<https://www.aacademica.org>.



Departamento Pedagógico de Contabilidad

**XII Jornadas de Investigación y Reflexión de Temas Contables  
en las Cátedras**

**3 y 4 de Noviembre del 2010**

**Salón de Utilidades Múltiples (SUM)**

**Área: Ejercicio Profesional**

*Título del trabajo*

ANÁLISIS DE LAS APLICACIONES INFORMÁTICAS DE  
CONTROL INTERNO EN ENTIDADES BANCARIAS PARA LA  
DETECCIÓN Y PREVENCIÓN DE LAVADO DE DINERO. (\*)

Elsa Beatriz Suarez Kimura  
Doctora UBA – Área Contabilidad  
Directora Proyecto UBACYT E034  
pkimura@econ.uba.ar

Diego Sebastián Escobar  
Contador Público – UBA  
Becario Maestría UBA  
escobards@gmail.com

(\*) Esta presentación ha sido financiada por el proyecto UBACYT E034 – 2008-2010 denominado Desarrollo de programas de formación ética y tecnológica para los profesionales de Ciencias Económicas: un modelo estratégico para la detección de actividades ilícitas y/u operaciones sospechosas (fraude y lavado de dinero).

Directora: Elsa Beatriz Suarez Kimura Doctora UBA – Área Contabilidad

## **ÍNDICE TEMÁTICO**

0. Resumen.
1. Introducción.
2. Recomendaciones del GAFI en relación a entidades financieras.
3. Controles Automatizados
  - 3.1. Características de los Controles Automatizados.
4. Características de las aplicaciones informáticas.
5. Importancia de la implementación de aplicaciones informáticas.
  - 5.1. XM3
  - 5.2. SmartSoft
  - 5.3. Effidetect AML
  - 5.4. Herramientas ofrecidas por Oracle.
6. Conclusiones
7. Bibliografía

# **ANÁLISIS DE LAS APLICACIONES INFORMÁTICAS DE CONTROL INTERNO EN ENTIDADES BANCARIAS PARA LA DETECCIÓN Y PREVENCIÓN DE LAVADO DE DINERO.**

## **0. RESUMEN.**

En el marco de la Jornada de investigación y reflexión de temas contables en las cátedras sometemos al análisis el Software de aplicación utilizadas en entidades bancarias para la detección y prevención de lavados de dinero.

Del mismo modo que evolucionaron los fraudes y delitos cometidos en las organizaciones, se implementaron con mayor rigidez los controles en las mismas. Gracias a las nuevas tecnologías disponibles en el mercado, se puede incrementar los controles, con la posibilidad de automatizarlos estableciendo parámetros para los distintos criterios de evaluación.

Los controles automatizados están cada vez más presentes en las organizaciones, por ejemplo, cuando una persona desea extraer de un cajero automático una suma mayor a la estipulada por el banco, si el sistema detecta un error en la transacción se impide la realización de la misma.

El objetivo del presente trabajo es informar a los profesionales en Ciencias Económicas, en especial al Contador Público, de los aplicativos informáticos utilizados por entidades bancarias en América Latina disponibles en el mercado, para efectuar controles permanentes en sistemas de información para detectar posibles operaciones relacionadas con “lavado de dinero”.

En la primera sección se analizarán las características de los controles automatizados y del software en cuestión, la implementación y su capacidad de establecer alertas relacionados con las operaciones registradas en entidades bancarias.

En una segunda parte se analizarán los productos disponibles en el mercado en relación, las plataformas de cada una. Algunos incluyen soluciones para prevención de lavado de dinero para intermediarios bursátiles.

En la última sección se analizarán arribarán a las conclusiones pertinente en el uso de esta tecnología en relación con la prevención de lavado de activos.

# **ANÁLISIS DE LAS APLICACIONES INFORMÁTICAS DE CONTROL INTERNO EN ENTIDADES BANCARIAS PARA LA DETECCIÓN Y PREVENCIÓN DE LAVADO DE DINERO.**

## **1. INTRODUCCIÓN**

En el marco de la Jornada de investigación y reflexión de temas contables en las cátedras sometemos al análisis el Software de aplicación utilizadas en entidades bancarias para la detección y prevención de lavados de dinero.

Del mismo modo que evolucionaron los fraudes y delitos cometidos en las organizaciones, se implementaron con mayor rigidez los controles en las mismas. Gracias a las nuevas tecnologías disponibles en el mercado, se puede incrementar los controles, con la posibilidad de automatizarlos estableciendo parámetros para los distintos criterios de evaluación.

Los controles automatizados están cada vez más presentes en las organizaciones, por ejemplo, cuando una persona desea extraer de un cajero automático una suma mayor a la estipulada por el banco, si el sistema detecta un error en la transacción se impide la realización de la misma.

El objetivo del presente trabajo es informar a los profesionales en Ciencias Económicas, en especial al Contador Público, de los aplicativos informáticos utilizados por entidades bancarias en América Latina disponibles en el mercado, para efectuar controles permanentes en sistemas de información para detectar posibles operaciones relacionadas con “lavado de dinero”.

La mayoría de las herramientas informáticas de control brindan documentación de procesos y el cumplimiento de diversa normativa nacional e internacional, como las leyes estadounidenses Sarbanes-Oxley y “USA PATRIOT ACT”, como también el Acuerdo de Basilea II.

Destacamos un informe realizado por Fondo Monetario Internacional, se han identificado más de 200 formas de “lavar dinero” en el mundo<sup>1</sup>, las cuales van desde la creación de fondos para apoyar actividades terroristas y la venta de drogas ilegales, hasta el fraude para evasión de impuestos. Según cifras de citado informe, entre 2% y 5% del producto interno bruto (PBI) mundial proviene de operaciones relacionadas con “lavado”.

Como se ha desarrollado en diferentes informes publicados<sup>2</sup> en el Centro de Modelos Contables (CECONTA), la ley en la República Argentina penaliza el lavado de activos y el encubrimiento, por lo cual consideramos de importante el conocimiento de estas nuevas herramientas del control para cumplir con la normativa nacional legal e internacional vigente.

---

<sup>1</sup> Fondo Monetario Internacional (2010), "Las soluciones informáticas no sólo cumplen un papel fundamental en la detección de transacciones ilícitas, sino que reducen los costos operacionales y garantizan el cumplimiento de normas internacionales" accedido desde <http://www.oracle.com>.

<sup>2</sup> Proyecto UBACYT E-034, Elsa Beatriz Suarez Kimura, UBACYT E034 – 2008-2010 denominado “Desarrollo de programas de formación ética y tecnológica para los profesionales de Ciencias Económicas: un modelo estratégico para la detección de actividades ilícitas y/u operaciones sospechosas (fraude y lavado de dinero).”

En este trabajo se analizan las características de los controles automatizados en las organizaciones y luego se observarán distintos aplicativos utilizados por entidades bancarias en América Latina.

## **2. RECOMENDACIONES DEL GRUPO DE ACCIÓN FINANCIERA (GAFI) PARA ENTIDADES FINANCIERAS.**

La Grupo de Acción Financiera (GAFI) emitió recomendaciones de para diferentes tipos de organizaciones para detectar y prevenir operaciones relacionadas con el lavado de activos. A continuación analizaremos exclusivamente las recomendaciones para entidades financieras.

En el apartado B del documento disponible en la Unidad de Información Financiera en la República Argentina, se establecen las medidas que deben tomar Instituciones Financieras y Actividades y Profesiones no financieras para impedir El Lavado de Activos y el Financiamiento del Terrorismo<sup>3</sup>.

La primera cuestión planteada en el pliego establece que los países deben asegurarse que las leyes de confidencialidad de las instituciones financieras “*no impidan la implementación de las Recomendaciones del GAFI*”.

*En relación con las entidades financieras* se recomienda que “*no deberían mantener cuentas anónimas o cuentas bajo nombres evidentemente ficticios*”. Las instituciones financieras deberían tomar medidas para llevar a cabo procedimientos de debida diligencia respecto del cliente, entre ellas la identificación y verificación de la identidad de sus clientes, cuando:

- Se inicien relaciones comerciales;
- Se lleven a cabo operaciones ocasionales: (i) por encima del umbral designado aplicable; o (ii) que sean transferencias electrónicas en las circunstancias cubiertas por la Nota Interpretativa de la Recomendación Especial VII;
- Exista la sospecha de lavado de activos o financiamiento del terrorismo; o
- La institución financiera tenga dudas acerca de la veracidad o congruencia de la información de identificación del cliente obtenida anteriormente.

“*Las medidas a tomar sobre procedimientos de debida diligencia respecto del cliente, son las siguientes:*

- a) *identificar al cliente y verificar su identidad empleando documentos, datos e información de una fuente independiente y confiable;*
- b) *identificar al beneficiario final, y tomar medidas razonables para verificar la identidad del beneficiario final de modo que la institución financiera quede convencida de que*

<sup>3</sup> GAFISUR Grupo de Acción Financiera de Sudamérica, (2003), “Las cuarenta recomendaciones GAFI”, accedido desde [http://www.uif.gov.ar/documentos%20GAFI/40rec\\_es.pdf](http://www.uif.gov.ar/documentos%20GAFI/40rec_es.pdf).

*conoce al beneficiario final. En el caso de las personas jurídicas y otras estructuras jurídicas, las instituciones financieras deberían, además, tomar medidas razonables para conocer la estructura de propiedad y control del cliente;*

- c) *obtener la información sobre el propósito y la naturaleza de la relación comercial;*
- d) *llevar a cabo un proceso continuo de debida diligencia respecto de la relación comercial, así como un examen detallado de las operaciones realizadas durante todo el curso de esa relación, con el fin de asegurar que las operaciones que se están haciendo son compatibles con lo que la institución sabe del cliente, sus negocios y perfil de riesgo, incluso el origen de los fondos, en caso necesario.*

*Las instituciones financieras deberían aplicar cada una de las medidas sobre procedimientos de debida diligencia respecto del cliente de los puntos a) a d) anteriores, pero podrán determinar el alcance de esas medidas sobre la base de la sensibilidad al riesgo, según el tipo de cliente, relación comercial u operación. Las medidas que se adopten deberían ser coherentes con cualquier pauta dictada por las autoridades competentes. En lo que hace a las categorías de mayor riesgo, las instituciones financieras deberían llevar a cabo un procedimiento de debida diligencia más exhaustivo. En algunas circunstancias en que los riesgos sean menores, los países pueden decidir que las instituciones financieras pueden aplicar medidas más reducidas o simplificadas.*

*Las instituciones financieras deberían verificar la identidad del cliente y del beneficiario final antes y mientras se establece una relación comercial o se hacen operaciones con clientes ocasionales. Los países pueden permitir a sus instituciones financieras que completen la verificación lo antes posible después de establecida la relación, cuando los riesgos de lavado de activos se estén manejando con eficacia y cuando sea esencial para no interrumpir el curso normal de los negocios.”<sup>4</sup>*

En los casos en que la institución financiera no pueda cumplir con lo previsto en los citados puntos (a) a (c), no deberían abrir cuentas, iniciar relaciones comerciales ni llevar a cabo la operación; o debería poner fin a la relación comercial; y debería considerar hacer un reporte de operaciones sospechosas (ROS) en relación con el cliente.

Estos requisitos se aplicarían a todos los clientes nuevos, aunque las instituciones financieras también deberían aplicar esta Recomendación a los clientes ya existentes en base a su importancia y riesgo, y deberían llevar a cabo un procedimiento de debida diligencia respecto de esas relaciones existentes en su debido momento.

Analizando estas recomendaciones resulta se suma importancia que las entidades bancarias refuerzen los controles en la detección de actividades sospechosas. A continuación se desarrollarán las características más relevantes de los controles automatizados.

---

<sup>4</sup> GAFISUR Grupo de Acción Financiera de Sudamérica, (2003), “Las cuarenta recomendaciones GAFI”, accedido desde [http://www.uif.gov.ar/documentos%20GAFI/40rec\\_es.pdf](http://www.uif.gov.ar/documentos%20GAFI/40rec_es.pdf).

### **3. CONTROLES AUTOMATIZADOS**

Los controles “automáticos” o “automatizados”, implementados por medios tecnológicos, permiten robustecer las evidencias llamadas de “auditoría” que podrían asegurar el correcto procesamiento de la información, por la persona adecuada, en tiempo y forma solicitada. Estas herramientas informáticas permiten a su vez integrar y centralizar operaciones de negocios, monitorear transacciones y validar controles internos.

Los controles automáticos permitirían

- Integrar y centralizar operaciones de negocios
- Monitorear transacciones
- Validar controles internos
- Documentar procesos y apoyar el cumplimiento

El uso de los controles automáticos en la detección de operaciones sospechosas en entidades bancarias permitiría la detección o llamada de atención de las mismas.

#### **3.1. Características de los Controles Automatizados**

Las principales características de los controles automáticos se detallan a continuación:

<b>CARACTERÍSTICAS DE LOS CONTROLES AUTOMATIZADOS</b>	<i>Disminución de la Intervención humana</i> <i>Disminución de uso de papeles</i> <i>Lógica de auditoria</i> <i>Evidencia Documental</i> <i>Recupero de información</i>
---	---

#### **“Intervención humana”**

*Al ser procesamiento automático, se disminuye la intervención humana, por ende, la posibilidad de error involuntario es menor.*

### **Disminución de uso de papeles**

*Al necesitarse menor volumen de evidencia de auditoría, de realizar procesamiento automático e ingreso de información directa, disminuye el uso de papeles y colabora en la disminución de la contaminación.*

### **Lógica de auditoria**

*En la actualidad, el 99% de los aplicativos posee la funcionalidad del resguardo de las operaciones realizadas durante el día, conteniendo los siguientes datos: Fecha y Hora, Usuario creador, Usuario Autorizador, Monto de la operación, Acciones realizadas, etc.*

### **Evidencia Documental**

*Al ser controles automáticos, la evidencia de resguardo sería electrónica y no física. Del mismo modo, con una sola copia de la evidencia es suficiente, y no es necesario una muestra de XX cantidad de casos, usados para validar controles manuales.*

### **Recupero de información**

*Al realizar el procesamiento bajo ambiente computarizado, y el resguardo en memorias o backups, el recupero y en consiguiente, el reprocesamiento de la información es mayor.<sup>5</sup>*

## **4. IMPORTANCIA DE LA IMPLEMENTACIÓN DE APLICACIONES INFORMÁTICAS.**

Una de las soluciones llevados a cabo por el sector financiero y diversas organizaciones internacionales en contra del lavado de dinero, ha sido la adopción de diferentes herramientas de monitoreo de actividades sospechosas, con el objetivo de automatizar los controles en este tipo de operaciones.

Las soluciones tecnológicas existentes en el mercado, en especial las de inteligencia de negocios como Anti Money Laundering (AML, desarrollada por oracle), ayudan a los bancos a detectar rápidamente operaciones ilícitas, a un costo más bajo, centralizando los datos, administrando y almacenando información financiera de clientes y sus transacciones, identificando patrones relacionados con operaciones de lavado de dinero, y entregando reportes de excepciones y alarmas que analizan los datos almacenados.<sup>6</sup>

Las soluciones informáticas facilitan el control y la auditoría de las transacciones, preparando a las instituciones para la adopción de políticas anti-lavado, a bajos costos operacionales. Las instituciones bancarias y financieras no sólo se protegen ellas mismas de los movimientos de dinero ilícito, sino que se hacen partícipes de una tarea global en la que están involucrados organismos mundiales, tanto privados como estatales, que trabajan por erradicar operaciones ilícitas que perjudican a la economía internacional.

---

<sup>5</sup> Scutella J. F., Barg V.E., (2010) RIESGOS DEL USO DE AMBIENTES COMPUTARIZADOS, "18º Congreso Nacional de Profesionales en Ciencias Económicas" Editorial Buyatti.

<sup>6</sup> ORACLE, (2010), Oracle Press Release "Herramientas para combatir el lavado de dinero" accedido desde <http://www.oracle.com>.

## **5. APlicativos más usados en el Mercado Latinoamericano.**

A continuación comentaremos las aplicaciones informáticas más utilizadas en el mercado latinoamericano:

### **5.1. XM3.**

El software XM3 fue diseñado por líderes de la industria en las áreas de detección de lavado de dinero, administración de riesgo, análisis de comportamiento humano, reconocimiento de patrones, y tecnologías de información. XM3 fue diseñado para ser rápido, confiable, seguro, fácil de implementar y utilizable en una variedad de ambientes.<sup>7</sup>

XM3 facilita el análisis de altos volúmenes de información y detecta escenarios y patrones de comportamientos complejos, inusuales, y sospechosos. El procesamiento se realiza por lotes o en tiempo real. XM3 puede leer información transaccional y de clientes directamente de los sistemas de las instituciones financieras sin requerir un componente intermedio que acumule y almacene la información (como puede ser un almacén de datos). Después de que la información es leída, se aplican una avanzada serie de métodos analíticos dentro del XM3 que detectan actividad inusual o sospechosa. Basados en la política de administración de riesgo de la Institución Financiera y en su aversión al riesgo, la actividad inusual se califica utilizando un método integral de administración de riesgo. La actividad calificada por encima de los umbrales definidos por la institución genera alertas que son presentadas al personal de cumplimiento para su revisión.

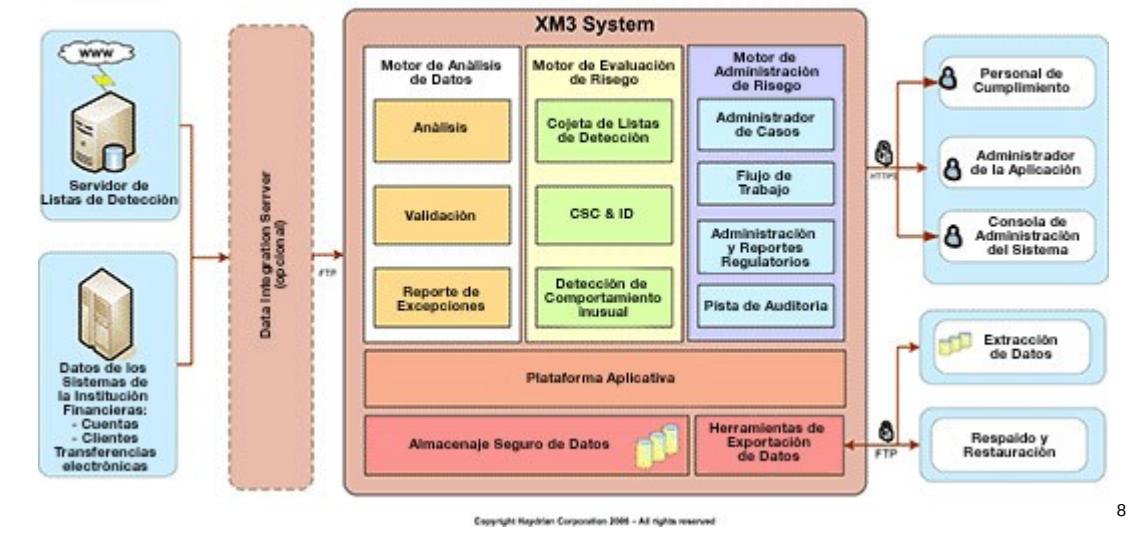
El Administrador de Casos XM3 ofrece avanzadas herramientas de flujo de trabajo y de trabajo en grupo para facilitar la investigación eficiente de las alertas. Debido a que los distintos bancos tienen distintas líneas de negocio, distintos tipos de clientes, y distintos riesgos potenciales, XM3 ha sido diseñado con distintos modelos analíticos de detección de amenazas.

Los modelos de detección que son apropiados para cada institución se determinan después de un concienzudo análisis de necesidades. Los distintos modelos que pueden ser implementados son:

- Conozca a Su Cliente (CSC)
- Cotejamiento de Listas de Detección
- Categorización por Perfiles de Comportamiento Histórico
- Comparación entre Pares
- Efectivo Estructurado y Actividad Equivalente
- Tránsito de Fondos
- Circulación de Fondos

<sup>7</sup> Haydrian (2010), "Prevencion de lavado de dinero para la banca", accedido desde <http://www.haydrian.com/PageID/374/default.aspx>

## Haydrian XM3 - Arquitectura del Sistema



### 5.2. SmartSoft.

Se trata de un *software* diseñado por la empresa costarricense Sentinel Compliance & Risk - SmartSoft para detectar operaciones relacionadas con lavado de dinero.

Esta solución monitorea en tiempo real las operaciones de todos sus clientes, genera un historial transaccional y lo compara con el perfil declarado. Adicionalmente, cuenta con una serie de reglas de experto (que permiten determinar actividades sospechosas típicamente asociadas con el lavado de dinero), como por ejemplo hacer varias transferencias en menos de una hora. Estas no solo incluyen los parámetros de la normativa nacional, sino también el conocimiento acumulado por la empresa en los otros 13 países en los que está presente.

Este aplicativo se apoya en las listas negras de las instituciones financieras anti-lavado de dinero a nivel nacional e internacional, como las de la oficina del control de activos extranjeros de Estados Unidos.

En el caso que se produzca una actividad inusual y sospechosa, de acuerdo con criterios escogidos por la institución financiera, el sistema dará una alerta y generará reportes regulatorios en los formatos solicitados por el ente regulador de cada país.

Este *software* incluye un apartado de excepciones para determinadas épocas del año o tipos de negocio. Por ejemplo, no genera alertas cuando una tienda de juguetes registra un alza en sus ingresos en fechas cercanas a la Navidad o el día del niño. “El sistema tiene niveles de seguridad por medio de roles y privilegios para que no todos puedan ver toda la información de cada cliente, y también indica cuál analista le está dando seguimiento a qué cliente, para la auditoría interna de la empresa”.

### 5.3. Effidetect AML.

<sup>8</sup> Haydrian (2010), “Arquitectura del sistema - XM3”, accedido desde <http://www.haydrian.com/PageID/374/default.aspx>

El software “effidetect AML” es desarrollado por la empresa Predisoft, como los demás aplicativos para prevenir y detectar operaciones relacionadas con lavado de dinero. A diferencia de las otras opciones en el mercado, no utiliza redes neuronales ni árboles de decisión para detectar los comportamientos inusuales, sino que utiliza un modelo matemático, para detectar atipicidades en el comportamiento de los clientes, es decir, movimientos que se distancian de su perfil declarado y de su historial transaccional.

Esta solución es más económica en el mercado y poseen un esquema de licenciamiento y mantenimiento diseñado para adaptarse al presupuesto de cada entidad.

#### **5.4. La alternativa de Oracle<sup>9</sup>.**

La empresa Oracle, una de las grandes empresas a nivel mundial dedicadas a la implementación y mantenimiento de bases de datos y Software de gestión, desarrolló herramientas para detectar y prevenir movimientos sospechosos en cualquier instancia del proceso de transacción de operaciones.

Esta empresa presenta varias herramientas las cuales cumplen con una función determinada en la lucha contra el lavado de dinero:

- *Data Extraction, Transformation and Loading Tool:* captura la información desde los múltiples sistemas de procesamiento a la base de datos.
- *Data Modeling and Management:* modela y administra los datos mediante tablas y relaciones de información, lo que facilita el almacenamiento de la misma.
- *Data-mining:* ayuda a los clientes a detectar patrones de lavado de dinero.
- *End-user Querying and Report Oracle Discoverer:* se caracteriza por ser una herramienta para la formulación de preguntas orientadas al análisis de la información.
- *Workflow Engine & Email Notification, Documentation & Control:* es una completa herramienta de auditoría de la información.
- *E-learning:* es la suite de administración de enseñanza que habilita a las entidades a dar entrenamiento y soporte en línea.

## **6. CONCLUSIONES.**

---

<sup>9</sup> ORACLE, (2010), Oracle Press Release “ Oracle brinda las mejores herramientas para combatir el lavado de dinero” accedido desde [http://www.oracle.com/global/lad/corporate/press/2005\\_mar/oracle\\_lavado\\_dinero.html](http://www.oracle.com/global/lad/corporate/press/2005_mar/oracle_lavado_dinero.html)

Como se indicó en el presente trabajo, en un informe realizado por Fondo Monetario Internacional, se han identificado más de 200 formas de “lavar dinero” en el mundo, las cuales van desde la creación de fondos para apoyar actividades terroristas y la venta de drogas ilegales, hasta el fraude para evasión de impuestos.

Las entidades bancarias y financieras son unos de los entes controlados en la lucha anti-lavado de activos. Los controles basados en aplicaciones informáticas contribuirían a reforzar las medidas de control sobre operaciones inusuales, ya que tienen la característica de ejecutarse automáticamente una vez configuradas dentro de los parámetros previstos; para desarrollar informes, estadísticas y enviar alertas sobre movimientos sospechosos.

La implementación de controles automatizados, no sólo cumplen un papel fundamental en la detección rápida de transacciones ilícitas, sino que contribuyen a las entidades bancarias a:

- Reducir los costos operacionales de los controles,
- Cumplir con las normas internacionales o recomendaciones como las establecidas por el GAFI.
- Centralizar los datos, administrando y almacenando información financiera de clientes y sus transacciones,
- Identificando patrones relacionados con operaciones de lavado de dinero,
- Entregando reportes de excepciones y alarmas que analizan los datos almacenados.

Ante este panorama es necesario comprender y manejar las nuevas tecnologías para la identificación y evaluación de los riesgos de detección de actividades ilícitas consecuencia de las responsabilidades descriptas en la legislación vigente.

## **7. BIBLIOGRAFÍA**

Fondo Monetario Internacional (2010), "Las soluciones informáticas no sólo cumplen un papel fundamental en la detección de transacciones ilícitas, sino que reducen los costos operacionales y garantizan el cumplimiento de normas internacionales" accedido desde <http://www.oracle.com>.

GAFISUR Grupo de Acción Financiera de Sudamérica, (2003), "Las cuarenta recomendaciones GAFI", accedido desde [http://www.uif.gov.ar/documentos%20GAFI/40rec\\_es.pdf](http://www.uif.gov.ar/documentos%20GAFI/40rec_es.pdf).

Haydrian (2010), "Arquitectura del sistema - XM3", accedido desde <http://www.haydrian.com/PageID/374/default.aspx>

Haydrian (2010), "Prevencion de lavado de dinero para la banca", accedido desde <http://www.haydrian.com/PageID/374/default.aspx>

ORACLE, (2010), Oracle Press Release "Herramientas para combatir el lavado de dinero" accedido desde <http://www.oracle.com>.

ORACLE, (2010), Oracle Press Release "Oracle brinda las mejores herramientas para combatir el lavado de dinero" accedido desde [http://www.oracle.com/global/lad/corporate/press/2005\\_mar/oracle\\_lavado\\_dinero.html](http://www.oracle.com/global/lad/corporate/press/2005_mar/oracle_lavado_dinero.html)

Scutella J. F., Barg V.E., (2010) RIESGOS DEL USO DE AMBIENTES COMPUTARIZADOS, "18º Congreso Nacional de Profesionales en Ciencias Económicas" Editorial Buyatti.