

## Boletín Informativo / Febrero 2016 UPCLC/CFT

### Tema: Cómo Prevenir y Detectar el Fraude

#### Prevención

Consiste en desarrollar controles para impedir que las situaciones de fraude interno ocurran y reducir las oportunidades de uso sin autorización de los recursos de la organización. Dentro del espectro de controles de prevención de fraudes se incluye la revisión de referencias en procesos de reclutamiento de personal, establecer políticas, procedimientos y segregación de funciones claramente definida, mantener supervisión constante, entrenamiento en prevención de fraudes y cultura corporativa de gestión de riesgos.



## **Detección**

Dado que los sistemas de control pueden ser tarde o temprano evadidos, detectar actividades irregulares tan pronto como sea posible es extremadamente importante. Para ello, la detección aplica controles diseñados para alertar al personal apropiado cuando se presentan circunstancias asociadas con actividades fraudulentas. Esto incluye desde mecanismos de auditoría interna hasta canales directos para reportar fraudes de manera anónima. Existen herramientas de detección computarizada que son capaces de revisar grandes volúmenes de datos, identificando patrones sospechosos en la data, aislando los casos que requieran de una investigación más detallada.

Además, existen metodologías y herramientas informáticas que ayudan a los auditores a identificar posibles situaciones de fraude interno, siendo el objetivo primordial el obtener evidencia suficiente para sustentar las situaciones irregulares detectadas y realizar sus recomendaciones.

## **Puesta en operación de los mecanismos de control**

Una vez que la organización conoce y ha definido políticas respecto a los riesgos y al perfil de los posibles perpetradores, debe implementar mecanismos que mitigarán el riesgo de fraude interno. Entre dichos mecanismos destacan:

- Definir e implantar una política funcional contra el fraude, que involucre a la unidad de tecnología de información con las demás unidades de la organización.
- Establecer las definiciones de controles de acceso y seguridad informática como parte vital de las políticas y procedimientos asociados a la tecnología de información, incluyendo la creación de la función de seguridad de activos de información.
- Definir e implantar contratos de responsabilidad del empleado, conocidos por todo el personal de todos los niveles de la organización.
- Mantener al tanto a los auditores externos de todos los riesgos presentes en la organización, incluyendo los proyectos en ejecución que tengan impacto sobre el ambiente de tecnología de información y el negocio.
- Definir e implantar un esquema de segregación de funciones y definición de roles y responsabilidades, donde el lineamiento principal sea que las funciones de adquisición de compromisos y la autorización de transacciones monetarias correspondientes, no descansen en un número limitado de personas.

- Implementar programas de inducción y entrenamiento orientados a crear una cultura organizacional de gestión de riesgos y prevención del fraude interno.
- Mantener canales de comunicación apropiados donde los empleados puedan reportar cualquier sospecha de manera anónima.

Es recomendable seguir ciertos lineamientos para fomentar la integridad y la ética de los empleados de la organización. Entre dichas acciones destacan:

- Definir y elaborar códigos de conducta debidamente divulgados, que involucren al personal de todos los niveles.
- Evitar la presión para cumplir con metas de rendimiento no realistas, por ejemplo situaciones en las que la presión está relacionada con resultados a corto plazo y donde la compensación está basada en lograr dichos objetivos.
- Descripciones de trabajo formales o informales que definan las tareas que comprenden trabajos específicos, debidamente comunicadas a los empleados, definiendo claramente las responsabilidades de cada individuo.
- Análisis del conocimiento y destrezas necesarios para realizar trabajos de manera adecuada, el cual es particularmente importante en el actual ambiente de tecnología de información, que cambia constantemente de manera vertiginosa.

Más allá de reforzar el ambiente de control interno, es primordial fomentar una cultura organizacional de altos estándares de integridad y ética, lo cual maximiza la acción de los mecanismos orientados a mitigar el riesgo de fraude. En ese sentido, acciones como las siguientes son recomendables:

- Puesta en operación de mecanismos de control apropiados en niveles ejecutivos
- Introducción de un código de conducta corporativo
- Aplicación pública de políticas de "cero tolerancia" y "no excepciones"
- Impulsar una investigación oportuna de fraudes e irregularidades
- Aplicar medidas disciplinarias de acuerdo al grado de la falta

## **FUNCIONES DEL DEPARTAMENTO DE PREVENCIÓN DEL FRAUDE**

La prevención del fraude es una obligación que atañe a toda la organización, al igual que sucede con la prevención del blanqueo de capitales y de la financiación del terrorismo, aunque con la diferencia de que esta obligación no responde a una materia de cumplimiento externo sino de control interno y, por tanto, estará sujeta a criterios basados en la escala de valores e intereses que tenga la empresa.

En algunas entidades financieras, durante muchos años el fraude ha estado camuflado dentro de la morosidad y asumido, por tanto, como un riesgo comercial más, controlable mediante políticas y procedimientos de análisis de riesgos comerciales o de recuperaciones.

Actualmente el fraude se analiza en el sector financiero como fenómeno independiente a la morosidad, y para ello, o bien se están creando los departamentos de prevención del fraude como estructuras especializadas, o se potencia su estudio dentro de la actividad ordinaria de otros departamentos, como los de seguridad, los de gestión de riesgos financieros, los de recuperaciones, etc.

Las entidades financieras que opten por la creación de estructuras especializadas como serían los departamentos de prevención del fraude, han que rentabilizarlas al máximo asignando a las mismas unos cometidos que estén acordes con la especialización de sus integrantes. Bajo mi criterio estos cometidos serían los siguientes:

- Control de la calidad y proporcionalidad de la base de datos de clientes
- Control operativo de la diligencia debida
- Coordinación de la investigación del fraude interno y externo
- Asesoramiento y apoyo a la acción reactiva de la empresa frente al fraude



## **Leyes y Entes que rigen el Fraude en Venezuela**

*El Código Penal Venezolano* en el **TITULO X De los Delitos contra la Propiedad, Capítulo III, artículo 462, De la estafa y otros fraudes**, reza así:

El que, con artificios o medios capaces de engañar o sorprender la buena fe de otro, induciéndole en error, procure para sí o para otro un provecho injusto con perjuicio ajeno, será penado con prisión de uno a cinco años. La pena será de dos a seis años si el delito se ha cometido: 1. En detrimento de una administración pública, de una entidad autónoma en que tenga interés el Estado o de un instituto de asistencia social. 2. Infundiendo en la persona ofendida el temor de un peligro imaginario o el erróneo convencimiento de que debe ejecutar una orden de la autoridad. El que cometiere el delito previsto en este artículo, utilizando como medio de engaño un documento público falsificado o alterado, o emitiendo un cheque sin provisión de fondos, incurrirá en la pena correspondiente aumentada de un sexto a una tercera parte.

Superintendencia Nacional de Valores (SUNAVAL)

### **Notas de Interés**

#### **Sistema Basado en Riesgos.**

De acuerdo con la recomendación N° 1 relativa a la Evaluación de riesgos y aplicación de un enfoque basado en riesgo emitida por el GAFI, así como, aplicar recursos encaminados para asegurar que estos se mitiguen eficazmente, se ha establecido un Sistema Integral para la administración de riesgos, a fin de disponer los recursos materiales y humanos necesarios para la supervisión y control en materias de prevención.

#### **Plan Operativo Anual de Prevención y Control de Legitimación de Capitales .**

Según artículo 21 de la resolución 110-11 del 19 de mayo de 2011, el sujeto obligado deberá diseñar anualmente un plan estratégico para prevenir y mitigar los riesgos de legitimación de capitales y financiamiento al terrorismo, este se encuentra conformado los siguientes aspectos; Actividades, Objetivo, Responsables, Unidad de Medida, Meta, Insumo, Costo, Tiempos de Ejecución.

## **Programa Anual de Adiestramiento**

Anualmente se elabora un "Programa Anual de Adiestramiento", ajustado a las características y funcionalidad de la Superintendencia Nacional de Valores especialmente dirigido para prevenir los riesgos de legitimación de capitales y financiamiento al terrorismo, este programa está dirigido a todo el personal, y puede ser realizado de manera interna o externa.

### **Plan Comunicacional.**

La resolución 110-11 del 19 de mayo de 2011, en su artículo 13 literal i el Oficial de Cumplimiento esta en la obligación de elaborar y difundir información en materia de prevención dirigidas al público, y a todo el personal de la institución conjuntamente con la oficina de Recursos Humanos.

### **Debida Diligencia**

La resolución N° 110-11 en sus artículos 31 y 44, contienen las disposiciones para implementar los procedimientos, medidas y controles internos para desarrollar adecuada y continuamente una Política de Debida Diligencia para el conocimiento tanto de propios y extraños.

### **Políticas sobre la visitas de Inspección**

En el artículo 58 de la N° 110-11 se plantea la obligación de ejecutar visitas de inspección a fin comprobar el cumplimiento de las disposiciones que minimizan la legitimación de capitales y financiamiento al terrorismo, como por ejemplo; Ley Orgánica Contra la Delincuencia Organizada y otras normas vigentes, serán efectuadas por los servidores públicos, especializados en este tipo de revisión y adscritos Sistema Integral para la Administración de Riesgos. La referida revisión debe priorizar la evaluación de la efectividad de los sistemas de monitoreo y detección de operaciones y/o actividades sospechosas de estar relacionadas con la legitimación de capitales y financiamiento al terrorismo

En cuanto a las ventanas para incorporar información relativa al lavados de Activos se presentan los siguientes:

Reporte de Actividades Sospechosas

Declaración Jurada de persona natural y jurídica

Ejercicios de Tipología

Denuncias y/o reclamos.

## **Algunos Ejemplos de Fraudes**

- *El robo o la malversación de fondos o valores*

El fraude piramidal denominado Ponzi, a menudo se incluyen nuevos inversores prometiendo invertir los fondos para generar altos rendimientos con poco o ningún riesgo. En muchos esquemas de Ponzi, los estafadores se centran en atraer nuevos fondos para hacer los pagos prometidos a los inversores en un corto periodo de tiempo; se utilizarán los recursos para cancelar gastos personales, en lugar de participar en cualquier actividad de inversión legítima, o para pagar altos intereses y atraer nuevos inversores que serán estafados, por cuanto no le pagaran, ni capital e intereses, es decir, todos ellos serán estafados.

- *Información privilegiada*

La manipulación puede implicar una serie de técnicas para afectar la oferta, o la demanda de una población. Estos incluyen: la difusión de información falsa o engañosa acerca de una organización; limitar indebidamente el número de valores disponibles al público para crear una imagen falsa o engañosa de la demanda de un valor. Los que participan en este tipo de manipulación están sujetos a diversas sanciones civiles y penales, por aprovecharse de la información privilegiada, ya sea verdadera o falsa.

Abuso de información privilegiada ilegal se refiere generalmente a la compra o venta de un valor, en violación de un deber fiduciario u otra relación de confianza y seguridad, mientras que en la posesión de información material no pública acerca de la seguridad. Violaciones de información privilegiada también pueden incluir la "propina" esa información, la negociación de valores por la persona "de punta", y la negociación de valores por los que se apropian indebidamente de dicha información.

- *Abusivo desnuda*

La venta en corto o al "desnudo", el vendedor no dispone de los valores al momento del pacto de la operación, debe comprar o pedir prestados los valores objeto de la operación momento de hacer la entrega al comprador. Como resultado, el vendedor no entrega valores al comprador cuando deba efectuarse la entrega (conocida como "la falta de entrega" o "a prueba").

**Con la contribución de todos podemos evitar el fraude a través del cumplimiento de unos sencillos tips informativos:**

- Suministrar todos los documentos y recaudos que soliciten al momento de realizar una apertura de cuenta.
- Informar el origen y destino de los fondos cuando los solicite.
- Mantener actualizados los datos (dirección, teléfonos, actividad económica, entre otros).
- Cualquier cambio en la información suministrada inicialmente, debe ser informada .
- Nunca dar información confidencial vía telefónica o correo electrónico a terceros o desconocidos.
- No permitir que terceros utilicen sus cuentas para realizar operaciones cuyo origen desconoce.

**Información extraída de la fuente:**

<https://temasdederecho.wordpress.com/2012/06/03/delitos-contrala-propiedad/>

<http://www.monografias.com/trabajos39/fraude/fraude2.shtml>

[http://www.sunaval.gob.ve/snv/slider2/legitimacion\\_cap.php](http://www.sunaval.gob.ve/snv/slider2/legitimacion_cap.php)

<http://www.iprofesional.com/notas/55368-Cmo-reducir-el-riesgo-de-fraude-en-las-empresas>

[http://serviciopreencionfraudeasnef.blogspot.com/2013/02/funciones-del-departamento-de\\_5070.html](http://serviciopreencionfraudeasnef.blogspot.com/2013/02/funciones-del-departamento-de_5070.html)

<http://unadocenade.com/una-docena-de-consejos-para-visitar-clientes/>

[www.mirelacion.es/blog/que-es-un-analisis-de-empresa/](http://www.mirelacion.es/blog/que-es-un-analisis-de-empresa/)

[www.gerenciaderecursoshumanosipc.blogspot.com/.../evaluacion-de-desempe...](http://www.gerenciaderecursoshumanosipc.blogspot.com/.../evaluacion-de-desempe...)