

**XI SEMINARIO NACIONAL DE SEGURIDAD
DEL SECTOR FINANCIERO**

MEMORIAS



ASOCIACIÓN BANCARIA
Y DE ENTIDADES FINANCIERAS
DE COLOMBIA

Presidente

César González Muñoz

Gerencia de Planeación y Proyectos

Director

Gustavo Ordóñez de los Ríos

Editor

Edgar Rubio

Coordinador Artes Gráficas

José Lucas Gutiérrez

Coordinación Publicaciones

María Clara Osorio

Diseño

Carlos González Bravo

Oliva Ortiz

Impresión

Fotomecánica Industrial

El contenido de esta Revista puede
reproducirse citando la fuente.

INDICE

RETROSPECTIVA DEL VII ENCUENTRO LATINOAMERICANO DE EXPERTOS EN SEGURIDAD BANCARIA

Luis Bernardo Quevedo Quintero..... 7

LA FISCALIA GENERAL DE LA NACIONA, UNA NUEVA REALIDAD EN COLOMBIA

Francisco José Sintura Varela 41

PAPEL DEL SECTOR FINANCIERO EN LA PREVENCIÓN Y CONTROL DEL LAVADO DE DINERO

Jorge Gabriel Taboada Hoyos 55

LINEAMIENTO PARA UN CODIGO DE CONDUCTA DEL SECTOR FINANCIERO

María Fernanda Guerrero Mateus 59

NUEVO CODIGO DE PROCEDIMIENTO PENAL	
<i>Guillermo Alvarez Peñaloza</i>	87
PLANES DE APOYO E INTERACCION DE LA POLICIA CON EL SECTOR FINANCIERO	
<i>Carlos Alberto Otálora Avendaño</i>	113
PREVENCION DE FRAUDES CON TARJETAS DE PAGO Y CHEQUES DE VIAJERO	
<i>Paul Bolívar</i>	129
ESTRUCTURA DE LA CAPACITACION Y EL SISTEMA DE DESARROLLO DE PERSONAL EN LAS EMPRESAS	
<i>Nelson Alvear Altamirano</i>	147
IMPORTRANCIA DE LA CAPACITACION EN LA VERIFICACION DE DOCUMENTOS DE VALOR	
<i>Hugo Salazar Marciales</i>	159
ADMINISTRACION DE RIESGO EN EL SECTOR FINANCIERO	
<i>Ernesto Clavijo Salgado</i>	167

INTRODUCCION

Anualmente se realiza el Seminario Nacional de Seguridad del Sector Financiero, evento que por tradición busca integrar las instituciones a través de sus representantes, y la discusión de temas de interés que sirvan de orientadores en las políticas y prácticas que deben tener dichas instituciones para el desarrollo normal y seguro de sus actividades.

Teniendo como escenario la ciudad de Villa de Leyva, el pasado 4 de diciembre se inauguró el XI Seminario Nacional de Seguridad del Sector Financiero. La instalación estuvo a cargo de los doctores Miguel Alvaro Mejía, Vicepresidente Operativo de la Asociación Bancaria y de Entidades Financieras de Colombia; y Fernando Silva Garcia, Superintendente Delegado de Establecimientos de Crédito de la Superintendencia Bancaria.

Esta reunión se presentó en momentos en que el país está atravesando una inicitada crisis social, cuyo asiento se encuentra en la descomposición moral, y sus efectos devastadores se manifiestan a través de los atentados terroristas dirigidos hacia todos los ciudadanos.

Algunas de las consecuencias han sido sufridas por las entidades financieras, motivo por el cual, existe la necesidad de que sus directivos, y en especial los

responsables de la seguridad, reaccionen de manera decidida en la búsqueda de soluciones integrales para enfrentar el problema.

Con el objeto de facilitar esa búsqueda, la Asobancaria a través de su Departamento de Servicios al Sector Financiero, invitó a funcionarios de cuatro áreas estratégicas de las entidades financieras a participar en este encuentro. Los invitados acudieron para compartir una agenda, que amplió el escenario en el que se ha desarrollado hasta hoy el evento. Para conseguirlo se trabajó en dos aspectos:

En primer lugar se pensó que, siendo la seguridad integral un tema que compete a todos, el seminario debería estar dirigido, no solo a los directores de seguridad, sino a funcionarios de otras áreas, como el Área de Personal, debido a que esta tiene bajo su responsabilidad la organización y dirección de un proceso de selección dentro de un marco que ofrezca seguridad sobre la idoneidad y honestidad del personal seleccionado y adicionalmente debe velar porque los funcionarios de la institución reciban la capacitación adecuada para poder desenvolverse ante los riesgos que enfrentan a diario; por otra parte, el Área de Operaciones debe tener pleno conocimiento de las estrategias y los mecanismos de seguridad dentro de los cuales realiza su trabajo, ya que con frecuencia se encuentran expuestos a la manipulación de operaciones fraudulentas por desconocimiento del empleado de las medidas de seguridad adecuadas, o negligencia de los mismos en el desarrollo de sus funciones; para el Área de Auditoría, resulta imprescindible tener una visión integral de la seguridad y contar con información oportuna y suficiente que le permita ejercer el control y gestión apropiados a través de la interacción con todos los empleados; en cuanto al Área de Seguridad, sobra decir que los temas de discusión fueron todos de su competencia. Esta área tiene bajo su responsabilidad el análisis de los Factores de Riesgo de la Entidad y el diseño e implementación de las medidas preventivas apropiadas. En otras palabras al Área de Seguridad le corresponde la Administración del Riesgo.

En segundo lugar se desarrolló un programa que incluyó los siguientes temas:

Una retrospectiva del VII encuentro Latinoamericano de Expertos en Seguridad Bancaria con el objeto de transmitir al interior del país las experiencias recogidas durante su realización en Guatemala el pasado mes de Septiembre. Se destacó la presentación de recomendaciones para la prevención y represión del lavado de dinero, basadas en acuerdos internacionales y en iniciativas internas de varios países.

Los resultados de la consideración de estos temas han tenido efecto en nuestra nación mediante la promulgación de recientes medidas de control, como es el caso de las establecidas mediante el Decreto 1872 de 1.992 y la Circular Externa 075 de la Superbancaria.

A continuación se presentaron 4 subtemas relacionados con el ámbito legal que se está desarrollando para combatir la delincuencia organizada, que utiliza el sistema financiero para encubrir sus operaciones fraudulentas. Al respecto se presentaron los lineamientos que se deben seguir para la creación de una Ley Marco para la prevención y control de los ilícitos⁽¹⁾; los cambios reales que se han dado en la legislación del país y el análisis de los mismos⁽²⁾; y las acciones concretas que se están desarrollando con aplicación de la nueva ley, para combatir a los infractores⁽³⁾.

De otro lado, se presentaron las actividades que viene adelantando la Policía para respaldar al Sector Financiero en la prevención de los delitos que se cometen contra el mismo⁽⁴⁾. Se destacó la creación de un nuevo sistema de

(1) *Maria Fernanda Guerrero*

(2) *Guillermo Alvarez Peñalosa*

(3) *Francisco Jose Sintura Varela, Jorge Gabriel Taboada*

(4) *Carlos Alberto Otálora*

alarmas que entrará a operar en 1.993, y un análisis estadístico de los asaltos a entidades financieras donde se profundiza sobre las causas que conducen a su realización.

Por último, se resaltaron la gestión administrativa y la capacitación como primeras herramientas para la prevención de los delitos contra el sector⁽⁵⁾. Se hizo énfasis en la importancia de la inducción y el entrenamiento de los funcionarios para lograr la efectividad en el trabajo. En este sentido se destacó el entrenamiento en presencia de clientes. Igualmente, se aludió a la comunicación como herramienta de primera mano en la prevención e investigación de estafas.

La XI versión del seminario se caracterizó por la concurrida asistencia y un elevado nivel en el tratamiento y discusión de los temas.

Durante el desarrollo del programa, en todas las conferencias persistió la idea de aunar esfuerzos para combatir al enemigo común: La delincuencia. Ese es el mensaje que nos deja el XI Seminario Nacional de Seguridad del Sector Financiero.

Nos queda la satisfacción de haber cumplido con los objetivos planteados desde el principio y reiteramos nuestros agradecimientos a todas las personas que abrieron un espacio en su agenda, para que este encuentro se hiciera realidad. La invitación es para mantener su interés en la Administración del Riesgo. La cita es en el XII Seminario Nacional de Seguridad del Sector Financiero.

(5) Paul Bolivar, Nelson Alvear, Hugo Salazar M., Ernesto Clavijo

RETROSPECTIVA DEL VII ENCUENTRO LATINOAMERICANO DE EXPERTOS EN SEGURIDAD BANCARIA

*Luis Bernardo Quevedo Quintero**

Quiero agradecer la oportunidad que me ha brindado la Asociación Bancaria y de Entidades Financieras de Colombia, por conducto de su Departamento de Servicios al Sector Financiero, dirigido por el Doctor Gustavo Adolfo Ordoñez para dirigirme a este grupo de personalidades interesadas en la Seguridad Bancaria. En esta oportunidad para presentar mis impresiones, sobre el Desarrollo del VII Encuentro Latinoamericano de Expertos en Seguridad Bancaria, realizado en la ciudad de Guatemala, durante los días 23, 24 y 25 de septiembre de 1992.

Es digno de destacar la concurrida asistencia de delegados procedentes de casi la totalidad de los países Latinoamericanos, con participación de representantes de Estados Unidos, Francia e Inglaterra, conformándose así, un grupo de aproximadamente 220 personas a las que habría que sumar los diferentes observadores del Gobierno de Guatemala que se hicieron presentes

*Jefe Dpto. de Seguridad Banco de Bogotá.

en el Certamen, exitosamente organizado por la Federación Latinoamericana de Bancos.

El Presidente de la Asociación de Banqueros de Guatemala, Licenciado Eduardo González Castillo, el Superintendente de Bancos en funciones, Licenciado Douglas Borja, el Presidente del Comité de Seguridad Bancaria de Guatemala, Capitán Mariano Escobedo y la Dra. Gloria Robayo de Duque, Asesora de Felaban hicieron la Inauguración, presentación de los expositores y dieron la bienvenida a todos los asistentes al Encuentro.

Para el desarrollo del Encuentro se programaron Once (11) temas, permitiéndose, al final de cada exposición que los asistentes realizaran las preguntas que consideraran pertinentes. El desarrollo de los temas fué el siguiente:

RETROSPECTIVA

- 1. Modalidades de siniestro más comunes, Ej. Delito interno, propuesta de solución y políticas.
Licenciado José Eduardo Martiguillo, Guatemala .**

Este tema fue orientado por el expositor hacia el fraude interno, realizado por empleados de los Bancos. Luego de efectuar la distinción entre fraude y estafa, concluye con que el fraude es una figura antijurídica mucho más amplia que la estafa debido a que abarca un sin-número de actividades que puede cometer el autor de un hecho ilícito para agenciarse patrimonio a través del engaño o ardid, tales como apropiaciones indebidas, abusos de confianza, en los que no es determinante que medie el ardid que provoca el error inicial, causante de la voluntad viciada, que caracteriza la Estafa.

1.1 Causas

Señala en primer lugar como **Causas Generales** la crisis moral, el ansia de riqueza, el desempleo, legislaciones inadecuadas, Auxiliares de Justicia improvisados, vigilancia oficial y particular carencia de preparación, entre otras.

Como **Causas Particulares** que predisponen a un empleado bancario a cometer hechos ilícitos en contra de su propia institución señaló: Conductas impropias del empleado, proliferación de sucursales, improvisación de funcionarios de seguridad, carencia de conocimientos de los empleados y temor para formular denuncias por parte de las Entidades afectadas.

Distingue como **Causas Concretas** los siguientes elementos:

- a) Que el empleado tenga un problema no compartible de naturaleza preferentemente económico.
- b) Conocimiento del empleado de que el cargo que se le ha confiado puede proporcionarle una fórmula para resolver el problema no compartible que le preocupa.
- c) Oportunidad de poder utilizar un ardid o engaño para obtener recursos económicos para su propio beneficio o de un tercero.
- d) Carencia de un adecuado control interno; y
- e) La impunidad.

1.2 Prevención del Fraude:

Por lo general el empleado que defrauda, es una persona que hasta antes de cometer su fechoría había sido honorable; no es un delincuente profesional, sino que al contrario es un delincuente ocasional. Esta reflexión induce a

afirmar al licenciado Marti Guillo que "La prevención encaminada a suprimir las ocasiones y las oportunidades mediante eficaces sistemas de control", es la manera más idónea de evitar esta clase de delitos. Sugiere tres sistemas:

- a) Contratación, selección e investigación del personal.
- b) Control Interno adecuado a las circunstancias actuales.
- c) Investigaciones técnicas y actuaciones judiciales.

1.3 Intervención del Fraude:

Por perfectos que sean los sistemas preventivos del fraude, es imposible evitar en su totalidad los manejos anormales del personal de una Institución Financiera. Estos empleados que se desadaptan en sus relaciones de lealtad con el Banco son peligrosos y es preciso descubrirlos.

Indica que aunque no existen técnicas ni reglas infalibles, toda investigación debe tener un plan de trabajo y una encuesta de ajuste, que no es más que una averiguación del método de vida que ha llevado el empleado desde que se realizó su selección e investigación hasta el momento en que surgió el problema.

Además de lo anterior, los investigadores deberán estar al tanto de los últimos procedimientos que se han realizado para cometer fraudes dentro de una Institución Bancaria, tales como:

- a) Adquisición fraudulenta de cheques genuinos y alteración de los mismos.
- b) Sustracción ilícita de formatos de cheques.
- c) Sustracción ilícita de formatos de Giros y de cheques de Viajero.

d) **Uso fraudulento de las terminales de computación:**

- Obtención ilícita de la clave de ingreso.
- El uso de terminales comunes sin seguridad de Ingreso.
- Eliminación de órdenes de no pago.
- Operaciones fraudulentas de notas de Crédito.
- Fraude mediante numerosas operaciones pequeñas.
- Fraude mediante una o pocas operaciones grandes, etc.

2. Lavado de Dinero: Lineamientos para la elaboración de un código de conducta y sus mecanismos de acción
Dra. María Fernanda Guerrero, Asociación Bancaria y de Entidades Financieras de Colombia.

En una muy documentada conferencia, expuso la Dra. Guerrero este tema, de relativa novedad en el mundo jurídico pero de gran actualidad e importancia en el sistema financiero universal, ya que de suyo hoy constituye una gran preocupación que las instituciones financieras sean utilizadas por la delincuencia organizada para lavar el dinero producto de sus actividades delictuales.

Abordó el tema haciendo un análisis de las iniciativas, recomendaciones y regulaciones para la prevención y represión del lavado de dinero adoptadas por organismos intergubernamentales en forma separada de las iniciativas de Derecho Interno, procedimiento que contribuyó a dar una mayor claridad.

En cuanto a las medidas adoptadas por organismos intergubernamentales profundizó en el contenido de los siguientes instrumentos:

- a) La Convención de las Naciones Unidas aprobada en Viena el 19 de Diciembre de 1988 (considera que el Blanqueo de Capitales debe combatirse principalmente con medidas de carácter penal y en el marco de la Cooperación Internacional, entre autoridades judiciales y policiales).
- b) Convenio del Consejo de Europa abierto a la firma el 8 de noviembre de 1990 en Estrasburgo cuyo enfoque es más amplio que el anterior instrumento en la medida en que considera que la estrategia contra el blanqueo de dinero no debe limitarse exclusivamente al enfoque penal, sino también desde la perspectiva del sistema financiero. Este enfoque lo desarrolló analizando las siguientes normas:
- Recomendación del Consejo de Europa, del 27 de junio de 1980.
 - Declaración de principios de Basilea, de Diciembre de 1988.
 - Directiva del 23 de marzo de 1990.
 - Directiva del Consejo de la C E E, del 10 de junio de 1991.
 - Recomendaciones del Grupo de Acción Financiera (GAFI).

Estas normas, entre otras, concretan los siguientes principios:

- a) Identificación plena de la clientela.
- b) Conservación de documentos para los efectos probatorios.
- c) Observancia de las Leyes y principios éticos.
- d) Colaboración con las autoridades judiciales.
- e) Compromiso de adhesión.

De la misma manera buscan concretar los siguientes aspectos:

- a) Tipificar como delito las operaciones que tengan como objeto el lavado de dólares.
- b) Imponer el deber de identificar tanto a los clientes habituales como ocasionales con operaciones superiores a \$14 Millones de pesos colombianos.
- c) Imponer al Banquero el deber de informar operaciones sospechosas a las autoridades.
- d) Establecer procedimientos adecuados de control interno.
- e) Capacitar a los banqueros para que puedan detectar operaciones de lavado de dinero y saber qué hacer o cómo proceder en estos casos.
- f) Abstenerse de ejecutar transacciones cuando estas sean sospechosas.

Explicó las recomendaciones de la Comisión Internamericana contra el abuso de las Drogas (CICAD) haciendo notar que el reglamento expedido por dicha entidad para el lavado de dinero:

- Afecta el Secreto Bancario ya que a su amparo se ocultan actividades y personas vinculadas al narcotráfico y otras formas del delito organizado.
- Dispone la extraterritorialidad de condenas o sentencias.
- Establece como deber de las Entidades Financieras el mantener únicamente cuentas nominativas.
- Establece la entrega de información Interestatal.

Sobre las iniciativas de Derecho Interno, analizó los mecanismos técnicos y jurídicos adelantados por la Asociación Española de la Banca Privada; las labores realizadas por la Asociación Bancaria Italiana; la Asociación de Bancos Franceses; las Estrategias Montadas por el Gobierno Canadiense y los mecanismos jurídicos de dos países Latinoamericanos: Panamá y Argentina.

Sobre la posibilidad de instrumentos jurídicos contra el lavado de dinero en Colombia, en primer lugar, informó sobre los procedimientos más usuales para lavar dinero a saber:

- Reintegro por exportaciones ficticias.
- Ingresos Personales
- Compra de divisas por ventanilla
- Inversión Extranjera camuflada a través de una Sociedad Constituida en el Exterior.

Y en segundo lugar, informó sobre el trámite del proyecto de Ley a través del cual Colombia se adhiere a la convención de Viena.

3. La estadística aplicada a la investigación de ilícitos bancarios Humberto Tagliabue Payán, Banco Nacional de México S.A.

El expositor enfocó su conferencia a explicar cómo el factor de competencia por ofrecer más servicios a la clientela, facilita la ejecución de ilícitos por parte de agentes externos o funcionarios de la institución. Esto ocurre porque la entidad disminuye los controles y los procedimientos de seguridad.

Presenta a continuación una complicada metodología de análisis de casos para concluir que las estadísticas debidamente codificadas y clasificadas de los

casos presentados conduce a identificar similitudes y, por consiguiente, a diseñar procedimientos que permitan robustecer la seguridad de las operaciones.

4. Interrelación o integración orgánica de las auditorías internas, los sectores investigativos, disciplinarios y los servicios de seguridad.

Licenciado Germán Parada, Asociación Bancaria de Venezuela.

En su exposición analiza el proceso evolutivo de la Auditoría Interna, la cual ya no consiste solamente en la evaluación de controles, sino que según las circunstancias deben averiguar, analizar, e inspeccionar abarcando un campo mayor a los aspectos financieros tradicionales.

Los equipos de seguridad bancaria deben ser asesores y por consiguiente, la relación entre Areas de Auditoría y de Seguridad debe ser íntima, comunicativa, cordial y respetuosa.

Sugiere que las investigaciones de seguridad se hagan sobre la base de buenas auditorías e invita a las Areas de Seguridad para que se pongan a tono con los adelantos tecnológicos para afrontar los retos que implican nuevos esquemas delictivos.

De acuerdo con las experiencias de su país considera que las Areas de Seguridad requieren comunicación con diferentes áreas de la organización y sustenta su punto de vista con estadísticas y flujogramas de comunicaciones entre las diferentes secciones con las cuales se comparten responsabilidades.

5. Estudios tendientes a la utilización de la informática en la detección de firmas falsas.

Licenciado José Balbuena Balmaceda, Seproban, México.

Inició su conferencia indicando cómo hace 50 años la mayoría de los Bancos de la región, llevaban las cuentas de sus movimientos en forma manual. Con los avances de la informática hoy, la mayoría de los empleados se dedican a la atención de la clientela porque las actividades de cálculo se realizan a través de la computadora. Por los años 40 las normas bancarias especificaban que para pagar un cheque, se debía previamente verificar que :

- Existiesen fondos.
- Comparar "Las firmas del archivo con la existente en el título valor". Si las formas de la firma coincidían efectuaba el pago.

En la actualidad el empleado bancario hace los cotejos con menos rigurosidad que antes... Ahora bien, desde sus comienzos el procedimiento ha sido ineficaz, porque a través de firmas falsas los Bancos han sido y siguen siendo víctimas de innumerables fraudes.

Antes, al igual que hoy, la respuesta a la pregunta de por qué suceden las estafas es la misma: "Las falsificaciones son perfectas y escapan a nuestra capacidad de detectarlas". Esta respuesta es tan aceptable que nuestras legislaciones consideran responsable al Banco, "sólo si la firma falsa es notoria o burdamente falsificada". En los estudios realizados se encontraron las siguientes causas de ineficiencia frente a las firmas:

- El método se limita al cotejo de las formas de las firmas.
- Las tarjetas están desactualizadas

-
- Los que cotejan desconocen las leyes fundamentales del cotejo técnico de firmas.

Por otra parte, no solo las falsificaciones perfectas nos engañan, sino también las burdas. Por qué? se han encontrado varias explicaciones:

- Se coteja prioritariamente las formas de las firmas, siendo lo que más varía en las firmas auténticas. Es imposible hacer dos firmas auténticas exactamente iguales.
- La forma es lo que mejor copian los falsificadores.
- Los visadores nunca han sido entrenados para "reconocer firmas falsas".

En la investigación adelantada por SEPROBAN sobre las características de los fraudes documentarios, se obtuvieron las siguientes observaciones:

- En todo fraude o estafa hay una falsedad.
- Si la falsificación es descubierta con oportunidad entonces el fraude se neutraliza.
- Las falsificaciones en documentos logran sus efectos, no tanto por la perfección de los imitadores sino por el total desconocimiento de quien los debe examinar.

Hace mucho tiempo se comprendió que la solución del reconocimiento de las firmas auténticas y falsas, comenzaría cuando se estuviese en capacidad de cuantificar una firma, lo cual creaba las siguientes dificultades:

- Es posible numerizar una firma?
- Cómo llegar a establecer "un número" para las auténticas, si estas poseen formas diferentes?

Para resolver estas cuestiones se realizaron estudios que permitieron encontrar elementos constantes, medibles y capaces de ser informatizados.

Si definimos la firma como "La forma gráfica que nosotros escogimos para identificarnos ante los demás" entonces reconocemos que hay elementos de reproducción automática que se encuentran gravados en el subconsciente, ellos determinan **los puntos de referencia intrínsecos**, tales como la proporción entre sus diseños, el intercalamiento de las presiones, los desenlaces, etc. y **los puntos de referencia extrínsecos**, por ejemplo la línea horizontal sobre la cual se escribe, o la antefirma de la cual se traza la firma y así por el estilo.

Es la constancia de nuestras reacciones frente a los puntos de referencia extrínsecos, lo que ha servido para encaminar los estudios que permiten la sistematización de estos datos.

Ahora bien. Cómo funciona el sistema informático en el cotejo de firmas? Primero, determina el patrón de variaciones de las firmas auténticas y luego cuantifica sus hábitos escriturales.

Establecidos los programas, se crean los ficheros sistematizados de firmas auténticas que servirán de patrón para los cotejos. Así, cada vez que una firma es sometida a cotejo, la computadora:

- Aplicará el mismo procedimiento empleado para memorizar las firmas auténticas, es decir: Las transformará en un conjunto de valores numéricos.
- Luego, verificará si estas concuerdan con los valores tenidos como auténticos.

Todos aquellos que escapen a dichos criterios, serán automáticamente rechazados.

Finalmente señaló las siguientes ventajas de este sistema:

- Disminución de la cadena burocrática,
- Rapidez del proceso,
- Visualización de los cotejos en caso de necesidad por pantalla.
- Las firmas rechazadas pueden ser objeto de reverificación.
- Actualización automática de los archivos de firmas auténticas.

6. La Seguridad Bancaria en un contexto de alta criminalidad y violencia. Mesa Redonda

Contralmirante Julio Raygada, Perú; Dn. Edilberto Carrioni, Colombia; Licenciado Roberto Antonio Canales, El Salvador ; Licenciado Adolfo Reyes Calderón, Guatemala;

Para el desarrollo de esta mesa redonda cada ponente expuso su punto de vista y posteriormente se dió a los asistentes la oportunidad de preguntar o contrapreguntar.

6.1 Licenciado Adolfo Reyes Calderón.

Definió conceptos sobre la Seguridad Bancaria, Violencia y Criminalidad para ubicar el marco teórico conceptual y proceder a realizar un análisis histórico de la violencia desde el punto de vista antropológico y luego desarrollar el concepto de criminología como fenómeno de la cultura indicando que los principales generadores de violencia son:

- La explosión demográfica, como generadora de Crisis Social y Económica.
- Los cambios Geopolíticos, que fomentan las guerras convencionales.

- Ciertas expresiones artísticas, que incitan a la violencia.

Pasando luego a ubicar en el caso centroamericano, concretamente en Guatemala, el fenómeno de la criminalidad violenta como factor de gran riesgo para la seguridad bancaria.

Señaló cómo en los últimos (5) cinco años los delitos violentos contra las instituciones bancarias en Guatemala han aumentado, estableciéndose según las estadísticas policiales que de veinticinco (25) Instituciones Financieras que operan en ese país, quince (15) de ellas han sufrido delitos violentos.

Se presentaron acciones de **Grupos Terroristas** haciendo terrorismo telefónico: Esto ha sucedido de manera cíclica y en momentos en que se presentan convulsiones de orden político, provocando evacuaciones, pánico y desórdenes dentro de las Instituciones que aún no contemplan dentro de la seguridad Institucional, planes de contingencia.

Actos violentos: únicamente se han registrado disparos, rompimientos de vidrieras causados por la delincuencia común. Sin embargo, se han presentado atentados contra la vida de los Ejecutivos de los Bancos.

Luego sentó las siguientes conclusiones sobre el caso Guatemalteco:

- La criminalidad violenta ha crecido en número de actos pero no en cuantía.
- Los delitos violentos provienen en su mayoría del Entorno Externo de los Bancos y los cuerpos de seguridad estatales no han tenido la capacidad de reprimirlos.

Finalmente, recomendó al Comité Bancario de Seguridad de cada país establecer un procedimiento por medio del cual pueda llevarse un control estadístico de todos los perjuicios materiales sufridos por los Bancos y

circular boletines "confidenciales sobre "MODUS OPERANDI", así como las medidas de prevención sugeribles, intercambiando información de criminalidad real y no de la aparente.

**6.2 Licenciado Roberto Antonio Canales Mantanilla,
Jefe de Seguridad del Banco Agrícola Comercial de El Salvador.**

Inició su intervención explicando que la Administración efectiva de los riesgos bancarios y la aplicación de las técnicas en materia de seguridad, han sido fundamentales para garantizar un ambiente en el cual las Instituciones Bancarias puedan ser siempre uno de los elementos importantes en el desarrollo de estos países.

Indicó que el Salvador tuvo 12 años de conflicto armado interno, período este que se caracterizó por el incremento de las acciones violentas. Contra la Banca se presentaron los siguientes crímenes:

- a) Secuestros de altos ejecutivos bancarios.
- b) Atentados con explosivos a numerosas entidades bancarias, con fines de sabotaje en horas nocturnas, que representaron grandes pérdidas materiales.
- c) Asaltos a sucursales bancarias, dejaron como consecuencia la muerte de miembros de la seguridad y la pérdida de cientos de miles de colones.
- d) Asaltos a unidades blindadas: se destaca el asalto de una unidad blindada, que transportaba cerca de US\$4 Millones hacia el Aeropuerto Internacional del Salvador, previamente planificado utilizando armas de grueso calibre que provocó la muerte de varios empleados, el año pasado.

- e) Cierre de sucursales bancarias: ante los fuertes combates que se desarrollaron en las localidades donde operaban, fue preciso cerrar varias sucursales bancarias por destrucción total de sus edificios.
- f) Amenazas telefónicas: estuvo de moda el sabotaje a los servicios bancarios utilizando este expediente, siendo importante anotar que varias de ellas fueron ciertas.
- g) Acciones vandálicas: como resultado de manifestaciones públicas que finalizaban en desórdenes callejeros, los delincuentes comunes se aprovecharon para:
 - Destruir fachadas, puertas y ventanales.
 - Incendiar vehículos blindados de propiedad de los Bancos.
 - Interrumpir las actividades laborales.
 - Agresión física a los guardas de seguridad.
 - Asalto a clientes después de efectuar sus operaciones bancarias.

Las Instituciones Bancarias salvadoreñas adoptaron las siguientes medidas ante estas condiciones de violencia generalizada:

- a) **Secuestros de Ejecutivos Bancarios:** Utilización de vehículos blindados, guardaespaldas, protección domiciliaria, implementación de comunicación privada, supervisión de visitas externas.
- b) **Atentados con Explosivos a Sucursales:** Retiro de vigilancia nocturna; instalación de puertas metálicas blindadas, eliminación de ventanales, protección interna de ventanales y divisiones de vidrio utilizando materiales antifrágidos.

-
- c) **Asaltos a Sucursales:** Supervisión de los sistemas de alarmas, instalación de Garitas, registro estricto de personas al ingresar a las sucursales bancarias, reducción al mínimo de las existencias de efectivo.
 - d) **Asaltos a Unidades Blindadas:** Traslados de efectivo a poblaciones remotas por transporte aéreo, utilización de garajes internos, cambios de rutina, comunicación interna, patrullaje en las zonas de desplazamiento.
 - e) **Acciones Vandálicas:** Instalación de vallas metálicas frente a las entradas, cierre inmediato de las oficinas, sistema adecuado de información respecto a las zonas de desplazamiento o manifestaciones.
 - f) **Asaltos a Clientes:** Retiro de las colindancias de los locales bancarios de todo tipo de vendedores ambulantes y personas sospechosas, patrullaje permanente en las zonas bancarias. Establecieron el sistema de fila única.

Consideró que en un ambiente de subversión y terrorismo, la debilidad mayor consiste en que las autoridades orientan sus recursos hacia la atención de la seguridad nacional y su respuesta ante las necesidades de protección de las instituciones financieras muchas veces no resulta oportuna, por lo que recomendó para los países en los que aún no exista, que los Bancos cuenten con sistema privado de patrullas.

Finalmente presentó el expositor unas reflexiones sobre los aspectos tratados indicando que en un ambiente de violencia generalizada sobre las instituciones bancarias, es importante conocer las amenazas a las que se hallan expuestas y las debilidades con que cuentan, para poner en práctica procedimientos de seguridad bancaria específicos ante eventos no tradicionales.

6.3 Contra-almirante Julio Raygada, Perú

Realizó una descripción de la violencia subversiva y actividad criminal generada por los grupos subversivos conocidos como Sendero Luminoso y Tupac Amarú y la criminalidad común como expresión de los complejos fenómenos económicos, sociales y políticos por los que atraviesa dicho país.

Señaló que en las 600 agencias bancarias ubicadas en el sector de las ciudades de Lima y Callao, durante el primer semestre de este año se presentaron 61 asaltos con un monto de siniestralidad cercano a los (US\$120) doce millones de dólares; se presentaron durante el mismo período 97 atentados terroristas con explosivos a agencias bancarias y 5 asaltos a vehículos transportadores de remesas, en uno de los cuales se alzaron con un botín cercano a los (US\$40) cuatro millones de dólares.

Ante esta situación coincidió con su antecesor en la apreciación de que las autoridades no tienen la capacidad de respuesta para afrontar el reto de tan alta criminalidad: "se viene produciendo una explosiva expansión de las actividades de la seguridad privada como una obvia respuesta de la ciudadanía para cubrir los requerimientos de protección de una población que se siente cada vez más desamparada", pero con las limitaciones de una industria incipiente, inexperta y poco preparada, refiriéndose al ámbito operativo de la seguridad física (policía de vigilancia).

Dentro de este marco la Asociación de Bancos del Perú ha canalizado esfuerzos para dotar adecuadamente a la Comandancia de Policía Nacional (comandancia Aguilas Negras) creada en 1992, para proteger en forma integral a las entidades bancarias, cubriendo tres campos específicos:

- Patrulla de vigilancia disuasión y reacción sobre locales bancarios.
- Custodia específica a pie de locales bancarios.
- Investigación e inteligencia de siniestros bancarios.

Estas medidas son complementadas internamente por cada banco a través de:

- Custodia de locales bancarios por medio de vigilantes.
- Administración de un sistema de supervisión cotidiana de las condiciones de seguridad en agencias y
- Habilitación de Artificios de seguridad tales como mecanismos de retardo y alarmas remotas conectadas a los servicios policiales o a servicios específicos de reacción privadas.

Pero todos estos esfuerzos aunque han dado resultado, son insuficientes. Señaló además que en el Perú es esencial que las Areas de Seguridad tengan mayor ingerencia en la administración de los siguientes aspectos:

- Control y Supervisión diaria de los niveles de caja.
- Administración de remesas de efectivo.
- Responsabilidades para funcionarios a cargo de agencias.

Finalmente expresó que es necesario un esfuerzo concertado de los bancos para dotar de una mayor seguridad la actividad bancaria en un contexto de alta presión criminal en los siguientes puntos:

- Tratamiento del acceso del público a los locales bancarios buscando una discreta individualización.
- Control operacional centralizado de niveles de caja en agencias.
- Administración operacional de un sistema de remesamiento de valores.
- Exigencia de disciplina y responsabilidad por aspectos de seguridad, a funcionarios, administradores, o jefes de agencias.

- Tratamiento corporativo de acuerdos estratégicos y tácticos con los organismos de seguridad oficiales.
- Jerarquización adecuada de los entes de seguridad en cada Banco.

6.4 Don Edilberto Carrioni López - Vicepresidente Contralor del Banco del Comercio de Colombia.

Realizó una síntesis de los aspectos tratados por cada uno de sus antecesores, presentando un juicioso y profundo análisis de los actos delictivos relacionados con los atracos, el terrorismo, el secuestro e indicando varias medidas previas de seguridad y vigilancia para tratar de disminuir su creciente actividad.

Luego de definir la seguridad como "La no existencia de peligro y una certeza de estar protegido ante éste", realizó algunas consideraciones sobre las actividades de los Departamentos de Seguridad y sus funciones, señalando que la seguridad es algo que no se puede improvisar, de ahí la necesidad de prevenir y disuadir. Siendo importante evolucionar teniendo en cuenta que es el área que analiza los riesgos y propone soluciones, que es mejor tener una sola debilidad y no todas. Haciendo entender a la Administración que las difíciles situaciones económicas en un país, hacen proliferar la actividad delictiva ya que sin el apoyo de la Alta Gerencia ningún programa de seguridad puede tener éxito por cuanto si el jefe no cree, el subalterno tampoco.

El crecimiento de la economía ha hecho proliferar oficinas que manejan un gran flujo de efectivo, atrayendo las bandas de atracadores, por lo que es indispensable adoptar medidas. Manifestó que para planear la seguridad de un Banco:

- Hay que identificar y evaluar los riesgos de las operaciones.

-
- Hay que identificar, evaluar y decidir los controles internos y de seguridad, y
 - Hay que hacer una relación sumaria de cuáles son los riesgos potenciales de los activos del Banco.

Luego de hacer un análisis sobre la clase de riesgos, los factores que afectan la seguridad física y las medidas que se deben adoptar, indicó que el Departamento de Seguridad debe estar totalmente orientado hacia la implantación de medidas de seguridad preventivas, correctivas e investigativas, dentro de una organización, contando con personal debidamente entrenado y experto en seguridades físicas o locativas, de protección a las personas e investigación.

En cuanto al terrorismo, manifestó que se trata de una de las mayores amenazas para la Industria Bancaria y se expresa a través de la extorsión, el secuestro, atracos y atentados en los que causan graves daños o se pierden grandes sumas de dinero, cuando se trata de actos contra oficinas bancarias o altos ejecutivos de la banca.

Realizó interesantes consideraciones sobre los grupos de terroristas, profundizando en la patología del terrorismo político y explicando sus estrategias indicó, que es muy difícil prevenir los actos terroristas y que solo con la participación de la comunidad haciendo causa común con las autoridades se podría controlar.

Por lo que se refiere a los atracos, en un medio de alta criminalidad y violencia, se manifiestan en cuanto a sus autores de 2 maneras: Los que son realizados por aficionados y los que son ejecutados por profesionales, siendo estos últimos a los que hay que dedicar mayor atención en la aplicación de medidas de seguridad en las cajas fuertes, en las casillas de los cajeros y en las bóvedas. Indicó que, entre otras, las medidas mínimas para prevenir atracos son:

- a) Crear condiciones que dificulten el acceso de los delincuentes y por consiguiente retrasar su acción.
- b) Crear un sistema de información automática en caso de intrusión a las bóvedas.
- c) Crear medidas que permitan la acción oportuna de la policía.
- d) Instalar en las puertas de las Cajas Fuertes cerraduras cronométricas.
- e) Instalación de cerraduras temporizadas en las bóvedas y cajas fuertes.
- f) Conexión de alarmas con la policía.

Señaló la importancia de la acción coordinada y mancomunada de las Asociaciones de Bancos con las Autoridades.

Indicó que una de las seguridades fundamentales es la de no exitar la codicia de los delincuentes manteniendo en las casillas de los cajeros altas sumas de dinero, sino únicamente la existencia indispensable para la atención a la clientela.

Luego explicó a los participantes algunos elementos de seguridad de uso en Colombia tales como cofres de efectivo en tránsito, recomendaciones para el recuento de remesas, protección de bóvedas, controles de acceso a las oficinas bancarias, instalación de cuartos de recuento, puertas de cajero y anclaje de cajas fuertes.

Advirtió que en caso de atraco, el personal de la oficina debe mantener la calma, no aumentar la tensión de los delincuentes y sobre todo, no provocar en ellos sobresaltos que puedan producir acciones indeseables.

Refiriéndose al secuestro, distinguió los de orden político de los realizados por delincuentes comunes. Indicó que hay que establecer medidas de seguridad muy severas para la custodia de los altos ejecutivos de la empresa, con instrucciones precisas a los familiares y a los encargados de la seguridad de cada Banco, para la intervención en caso de un insuceso. Recomendó la creación de un comité especializado para tomar medidas antes de que ocurra un hecho de esta naturaleza:

- Dictar o tener políticas para evitar improvisaciones ante situaciones de emergencia.
- Crear sistemas especiales de seguridad para proteger a los altos ejecutivos de la institución.

Insistió en la conveniencia de estar preparados para un atraco con toma de rehenes, haciendo ver la complejidad y el delicado manejo de estas situaciones. Luego recomendó a los encargados de la seguridad tener en cuenta los siguientes aspectos:

- Seleccionar a quién o a quiénes es indispensable vigilar.
- Convencer al funcionario, mediante una metódica labor de persuasión de los beneficios que estas medidas le reportan.
- La vigilancia antisequestro debe ser total.
- Blindaje del vehículo en que se desplace con escoltas.
- Reconocimiento periódico de sitios aledaños al sector donde está la empresa y la residencia del funcionario.

Luego realizó algunas consideraciones sobre el manejo de casos en los que se presenta toma de rehenes, indicando la importancia de estudiar todas las

posibilidades en que estos actos se puedan presentar, para cuando llegue el momento, poder dar un adecuado tratamiento a esta situación, cubriendo todas las etapas desde las medidas preventivas hasta cuando llegue la crisis. Exaltó el apoyo que puede brindar la policía en estos casos, sobre todo cuando el hecho ha ocurrido e insistió en que las **vidas humanas priman** sobre cualquier otro tipo de interés.

7. Seguridad Bancaria en informática y en los sistemas de transferencia electrónica de créditos
Señor Vadir del Cistia, Banco de Boston, Brasil.

Inició su conferencia indicando que existen diferentes clases de activos, entre los cuales se encuentra la información. Esta es un activo que también es objeto de atentados que pueden causar pérdidas catastróficas a las empresas. Si se analiza la composición de las amenazas contra los activos de una empresa se obtendría la siguiente:

Errores Humanos	60%
Descontento	10%
Deshonestidad	10%
Fuego	10%
Agua	7%
Agentes externos	3%

Esto significa que el 80% de las pérdidas de las empresas, son consecuencia de amenazas internas y ellas son causadas por personas. Se puede afirmar entonces, que los crímenes por computador son causados por personas comunes.

Señaló que la tendencia delincencial por computador va en aumento, razón por la cual es necesario definir como objetivos de protección la integridad, la exactitud y autorización.

Explicó que todo lo que nos lleve a perder dinero o a obtener un mal resultado es lo que llamamos **riesgo**, como por ejemplo: Decisiones erradas, mal uso de los recursos, exposición indebida y ataques externos.

Existen varias formas de ataques a la información e indicó la forma de protegerse:

- Personas que tratan de entrar al sistema, la protección es encriptar.
- Alteraciones de la información, la protección es un buen sistema de control.
- Alteraciones de código realizados por empleadores de centros de cómputo, la protección es un buen sistema de control.
- Virus, que son programas instalados en los computadores con capacidad de multiplicarse, la protección son vacunas y adecuados procedimientos.

De acuerdo con lo anterior, la protección cumple funciones detectivas para establecer que algo se está haciendo mal. Estas funciones deben aplicarse en los siguientes niveles de seguridad:

- Entrada al sistema (cliente)
- Perfiles de transacción
- Terminal por transacción
- Datos

Cada nivel de seguridad define niveles de control colocando por ejemplo, para entrada al sistema la implantación de claves, las cuales para que sean efectivas deben reunir los siguientes requisitos:

- Clave secreta individual
- Plazo de validez
- Debe componerse de caracteres alfanuméricos
- Mínimo de seis (6) posiciones.
- No debe contener letras del nombre del cliente.
- Debe ser diferente a cualesquiera de las tres (3) últimas claves utilizadas.

Finalmente, centró sus comentarios en la descripción del análisis de los perfiles de transacción haciendo las siguientes recomendaciones:

- a) Es necesario realizar análisis del flujo operacional en primera instancia.
- b) Implantar disciplinas de control tales como:
 - Segregación de funciones
 - Supervisión de operaciones.
 - Validación de la información.
 - Autorización de las operaciones.
- c) Los controles deben estar preparados al momento de:
 - La implantación del sistema.

- Inicio de un producto o servicio.

Señaló que estos aspectos deben quedar adecuadamente documentados mediante ficheros especiales.

8. Defraudación por duplicación y adulteración de documentos bancarios . Influencia del Laser, color y fotocopias
Señor Blas Emilio Noguera,
Comisión Argentina para Felabán, Argentina.

Inició su exposición advirtiendo que desde hace mucho tiempo se tuvo la voz de alerta con respecto a las fotocopiadoras a color, las cuales no solo han sido perfeccionadas dotándolas de elementos de mayor eficacia, sino que están en el mercado a costos más accesibles, incrementándose en consecuencia la posibilidad de la reproducción de documentos valorados mediante este sistema. Por esta circunstancia se efectuaron investigaciones tanto al papel como a la impresión.

Al papel le fueron incorporados distintos elementos dentro del proceso mismo de fabricación tales como filmillas, lentejuelas tanto visibles como invisibles y se adicionaron en su masa agentes químicos decolorantes.

A la impresión, se introdujeron tintas reactivas, fugitivas, con variaciones de color a la exposición a la luz natural, como a la luz ultravioleta.

Estos logros han creado una interesante barrera frente a esta modalidad delictiva. Sin embargo, considera que la utilización combinada de la Impresión Laser y las fotocopiadoras a color pueden lograr ejemplares de alta resolución y para demostrarlo profundizó en los diferentes aspectos técnicos químicos, ópticos y físicos explicando ampliamente la vulnerabilidad de todos los elementos incorporados a los documentos valorados. Luego expuso 2 métodos efectivos para contrarrestar todas estas maniobras indicando:

- Aplicar tintas de pigmentación metálica en las impresiones, ya que el brillo y reflexión que tienen no son reproducibles en las fotocopiadoras.
- La incorporación de la marca de agua durante el proceso de fabricación y la forma de llevarlo a cabo, es un factor determinante en la imposibilidad de reproducirlas.

La primera de ellas es la más técnica y solo es apreciable por expertos en la materia, la otra puede ser verificada por el tenedor del documento, por lo que es más recomendable aquella, ya que "No se copia lo que no se vé directamente".

9. Departamento de Manejo de Riesgos en la Banca: Objetivos, estructuras y funciones

Señor Alain Morizet, Banco de Comercio Exterior de Francia.

La evaluación de los riesgos a los que se enfrenta una empresa son competencia del Gerente de Riesgos, profesión muy novedosa especialmente en la banca si se define como un enfoque global, dinámico y agresivo de los diversos riesgos que enfrenta la banca, en vez de reducirlo, al manejo pasivo y defensivo de los riesgos y a su transferencia, dentro de lo posible, a las compañías aseguradoras.

Para explicar la función de un Departamento de Gestión de Riesgos definió rápidamente los dos tipos de riesgo que clásicamente se distinguen: **Los riesgos especulativos:** son los que resultan de las actividades normales de la empresa, son mensurables en sus efectos y controlables; **los riesgos puros:** son la consecuencia de eventos accidentales o aleatorios. Los riesgos puros son difícilmente delimitables y controlables.

Los riesgos puros han conformado tradicionalmente el campo de aplicación del "manejo de riesgos". Hoy en día se debe superar esta dicotomía (riesgos puros/riesgos especulativos), porque existe una creciente interdependencia entre ambas clases. Se observa por lo tanto una integración del manejo de

ambos tipos de riesgos dentro de las funciones del Departamento de Manejo de Riesgos.

En consecuencia la meta es la identificación de los riesgos, su cuantificación y la coordinación del conjunto de acciones que pretenden controlarlos (prevención, protección, seguros). Para ello, su función es reflexiva únicamente, no debe ejecutar ni pretender sustituir las directivas y servicios del banco. Su estructura es muy pequeña, se reduce a un titular y uno o dos colaboradores que reportan a la presidencia. Especificó los campos de acción de un Departamento de Riesgos así:

- Seguridad de bienes y personas
- Seguridad de sistemas
- Control interno
- Definición de las reglas deontológicas
- Definición de una política de seguros.
- Controlar los compromisos adquiridos por el banco.

Finalmente, afirmó que el objetivo de un Departamento de Manejo de Riesgos no es garantizar una total prevención de los riesgos que enfrenta un banco; esto sería una utopía, cero riesgos es algo que no existe.

10. Sistema de evaluación y corrección operativa de seguridad para personal de vigilancia extramuros e intramuros.

Capitán José Antonio Muñoz Prieto, Gerente Regional de SEPROBAN- México.

Inició su conferencia presentando el marco contextual de la elaboración de un programa para la supervisión, evaluación, concientización y corrección

del personal de vigilancia de SEPROBAN. Este programa lo denominan SECCO.

Sus características generales son:

- Racionaliza el desempeño del personal con los recursos disponibles.
- Proporciona información sobre el desempeño individual.
- Ofrece información para la toma de decisiones.
- Auxilio en el reconocimiento de la relación costo-eficiencia.
- Es un sistema flexible, pues permite al usuario estructurarlo de acuerdo con sus requerimientos.
- Hace visibles a todos los miembros del grupo los resultados de las desviaciones en su conducta.

Se definieron para el programa las siguientes áreas de actividades sujetas a control : Presencia, Asistencias, Patrullaje, Cuidado de las unidades y Capacitación. Cada una de estas actividades comprende variables que desarrollan su contenido.

El sistema SECCO opera con base a un programa computarizado, que concentra la información de las áreas de actividad y sus variables sujetas a control.

Diariamente se captura la información mediante reporte de los supervisores, de los datos referentes a las áreas de actividad bajo control. En la función de **evaluación**, se confrontan los datos obtenidos en la supervisión con los estándares de eficiencia establecidos. La **concientización** opera a través de :

a) Acciones:

- Información continua de los resultados obtenidos.
- Orientación, reuniones de trabajo y entrevistas a través de los supervisores y mandos medios.
- Capacitación para el desarrollo de los conocimientos y habilidades que requiere el servicio.

b) Medidas:

- Estímulos y reconocimientos periódicos.
- Promoción laboral.

La **corrección** está orientada a 2 aspectos presentes en el servicio. El Personal y los Recursos Materiales. Con respecto al personal, con base en la información obtenida, analizada y evaluada los elementos que durante tres meses seguidos permanecen en el nivel mínimo de desempeño y son retirados del servicio. Con respecto a los Recursos Materiales, estos son aprovechados adecuadamente en razón a que se cuenta con un grupo de guardias más eficiente.

Finalmente explicó que para SEPROBAN, este sistema ha representado una aproximación sistemática a la solución de la compleja tarea de administrar recursos humanos y materiales destinados a la seguridad externa e interna de las instituciones de crédito.

11. Protección de los altos ejecutivos bancarios.

Anthony J. Scotti , Estados Unidos.

Esta charla fue matizada por el expositor mediante la presentación de casos de la vida real concluyendo que en todo atentado solo es víctima el ejecutivo

que es más fácil de secuestrar, por inexistencia de medidas de seguridad. Indicó que en todo atentado hay un proceso de selección que cubre las siguientes etapas:

- a) El terrorista hace la lista de los secuestrables.
- b) En una segunda etapa, el terrorista procede a eliminar los blancos difíciles. Se tachan de la lista aquellos ejecutivos debidamente protegidos.
- c) Estudio de la información: Los datos recopilados sobre rutas, rutinas, escoltas, etc. son sometidos al más riguroso análisis, para escoger la víctima.
- d) Selección del Blanco: Como los terroristas toman el camino de la menor resistencia, es preciso asegurarse de ser el más fácil de secuestrar.

¿Dónde ocurren los ataques? Los sitios recurrentes en los casos de atentados contra importantes ejecutivos ocurren:

- En la casa de habitación y sectores aledaños: Los ejecutivos llegan temprano a su trabajo y no cambian las rutas porque pierden tiempo.
- En la oficina o cerca a la oficina: No se consideran diferentes, quieren actuar como los demás y desean atender a quien los necesite, sin tomar precauciones.

¿Qué hacer para lograr una adecuada protección? Lo primero es convencer al ejecutivo que requiere seguridad. Luego dedicar tiempo para identificar los puntos de riesgo. Establecidas las áreas de riesgo hay que examinar los sitios para determinar qué es lo normal en ellos, la más mínima variación debe ser objeto de investigación. Es obligación de los responsables de la seguridad

hacer que las comunicaciones con el ejecutivo funcionen para lograr que "si se nota algo extraño hay que avisarlo, si hay aviso hay que hacer algo".

12. Clausura

Leopoldo Salazar, Segundo Vicepresidente del Comité Latinoamericano de Expertos en Seguridad Bancaria.

Gloria Duque de Robayo, Asesora de la Federación Latinoamericana de Bancos (Felabán) quien agradeció a los conferencistas y asistentes al evento la colaboración que brindaron para el buen desarrollo de este.

Durante los tres (3) días que duró el evento estuvo a disposición de los asistentes la exposición de Equipos y Servicios de Seguridad y Controles presentados por veintiseis (26) expositores que mostraron los últimos avances en dispositivos y elementos de seguridad.

LA FISCALIA GENERAL DE LA NACION, UNA NUEVA REALIDAD EN COLOMBIA

*Francisco José Sintura Varela**

INTRODUCCION

Una de las batallas mas grandes que ha librado Colombia en su pasado mas reciente esta constituida por su lucha contra la impunidad. En esta lucha se ha buscado combatir diversos fenómenos que tradicionalmente han impedido el fortalecimiento de la administración de justicia, su modernización y eficacia. La falta de técnica en el adelantamiento de las investigaciones, las dificultades de carácter presupuestal, la acción depredadora del narcotráfico, la ausencia, a veces sentida de una amplia colaboración en el intercambio de información y de pruebas y de otras diversas causas han requerido un ataque frontal, no solamente por parte del gobierno si no de las demás instituciones y la ciudadanía, para ofrecer alternativas de solución que llevaran a una verdadera renovación institucional.

Lamentablemente, a la opinión internacional ha llegado la imagen de una justicia que se mira como impotente para adelantar el juzgamiento de los más señalados delincuentes y esa no es la realidad de nuestro país. Grande es

*Vicefiscal General de la Nación.

entonces el daño que se le hace no solo a Colombia, sino en general a toda América al ofrecerse una visión de un país de esa manera, olvidando la grandeza de un pueblo que ha ofrecido sus mejores vidas en la lucha contra la criminalidad y el terrorismo.

No obstante Colombia, país de honda tradición democrática, emprendió la lucha por su renovación institucional en el propósito de atacar uno de sus problemas más significativos: La credibilidad y fortalecimiento de su sistema judicial.

El proceso de cambio institucional emerge con la nueva Constitución de 1991, la cual dotó al **Estado de Derechos** de las armas suficientes para librar la lucha contra la impunidad y entregó a los ciudadanos los instrumentos necesarios para hacer efectivos sus derechos y asegurar el ejercicio de sus libertades.

En el propósito de fortalecer los instrumentos de la justicia, rodearla de seguridades y organizarla desde el punto de vista de su administración, se crearon en la Constitución nuevos entes que le aseguraran su función Pública permanente, autónoma e independiente, con un funcionamiento desconcentrado para garantizar el acceso de cualquier ciudadano a ella. Aparecen entonces la Corte Constitucional, a la que se confía la guarda y supremacía de la Constitución, el Consejo Superior de la Judicatura como máximo organismo de la administración de la justicia y la carrera judicial encargado del control de la gestión ética de la prestación del servicio de la justicia, así como el Defensor del Pueblo en su función de guardián y protector de los derechos humanos.

Por su parte, la Fiscalía General de la Nación, como integrante de la Rama Judicial pero con autonomía administrativa y presupuestal, se erige con la Nueva Constitución como la cabeza en la lucha contra la delincuencia y la impunidad.

LA FISCALIA GENERAL DE LA NACION

La Fiscalía se concibe en el marco de un sistema procesal mixto acusatorio, por lo que, en lo sucesivo, la tarea de investigar el delito o acusar a los delincuentes se asigna a los Fiscales y la de juzgar y condenar a los infractores de la ley penal, se encomienda a los jueces.

Como principio de actuación, la misma Constitución Política obliga a la Fiscalía a investigar tanto lo favorable como lo desfavorable al sindicado y a respetar sus derechos fundamentales y garantías procesales.

Este principio de legalidad se plantea igualmente en relación con los Fiscales Delegados a quienes corresponde velar porque el cumplimiento de las actividades asociadas con las funciones de investigación se adelanten de conformidad con el respeto por el derecho a la defensa, los derechos humanos y la prevalencia del derecho sustancial sobre el adjetivo.

Al Fiscal General, directamente o por conducto de sus delegados se atribuye la función de dirigir, controlar y coordinar el desarrollo de la función de legalidad e imparcialidad.

Importa destacar seguidamente, las razones de carácter práctico que imponen la creación de la Fiscalía, en el propósito de determinar sus características sustanciales, organización y funciones.

Quizá cuatro problemas fundamentales han aquejado la administración de justicia en Colombia, en el ámbito de su justicia penal: la jurisdiccionalización de los conflictos, la ineficacia de las investigaciones, el bajo rendimiento cuantitativo de los despachos judiciales y los fenómenos de violencia a los que tradicionalmente se ha visto expuesta. El primero de ellos se combate a través de los mecanismos de descongestión de despachos judiciales y la administrativización de comportamientos menos graves. Para los segundos se crea la Fiscalía General de la Nación y para controlar los fenómenos de

violencia, amén de la acción decidida del Estado, se requiere el concurso y apoyo de la comunidad en general.

En efecto, la ausencia de un esquema ágil de investigación, la dispersión en varios órganos de investigación del estado de las funciones de Policía Judicial, la limitación por el territorio de la competencia de los funcionarios de investigación, la inexistencia de controles internos sobre la gestión de los funcionarios judiciales, las dificultades de carácter presupuestal y la ausencia de un organismo al que se hiciera responsable por la protección de las víctimas, los testigos y demás intervinientes en el proceso penal, constituyen causas que dan nacimiento a la Fiscalía.

Esta se concibe bajo tres grandes principios: UNIDAD DE GESTION, UNIFORMIDAD DE ACTUACION Y CONTROL JERARQUICO. Ellos pretenden que la entidad asuma en una organización piramidal el manejo, coordinación y control de la administración de investigación, de tal suerte que los principios de autonomía e independencia judiciales, se conjuguen con los de unidad y jerarquía dentro de los límites de la legalidad y la imparcialidad.

La Fiscalía hace parte de la Rama Judicial y esta es quizá su característica diferenciadora con otros sistemas que adoptan esta institución. Sin embargo, tiene autonomía administrativa y presupuestal, hecho que se refleja en un régimen propio de carrera, de contratación, disciplinario, de bienestar social, de capacitación, en un todo, en un régimen propio de prestación del servicio público.

A la Fiscalía le compete por conducto de sus fiscales delegados, calificar las investigaciones, asegurar la comparecencia de infractores de la ley penal, tomar las medidas necesarias para hacer efectivo el restablecimiento del derecho, dirigir y coordinar las funciones de policía judicial, dirigir el intercambio de información y de pruebas en el ámbito internacional y velar por la protección de víctimas y demás intervinientes en el proceso penal.

LA FUNCION DE POLICIA JUDICIAL

Dentro de este panorama normativo, permítanme detenerme en la revisión sucinta de la función de Policía Judicial, en atención a la importancia que el tema reviste, si se considera que por mandato legal, el Fiscal General puede asignar funciones de ésta naturaleza en entidades públicas que ejerzan funciones de vigilancia y control.

Sea lo primero reiterar que la dirección, coordinación y control de toda actividad de policía judicial es atribución radicada en cabeza del Fiscal General, salvo la que compete a la Procuraduría General de la Nación, según lo dispuesto por el Artículo 277 de la Constitución Política.

Es esta la razón por la que el Fiscal General preside el Consejo de Policía Judicial, del que además hacen parte el Director del Departamento Administrativo de Seguridad, el Director General de la Policía Nacional, el Director del Instituto Nacional de Medicina Legal y Ciencias Forenses, el Procurador General de la Nación y el Contralor General de la República.

A dicho Consejo compete asesorar al Fiscal General en el establecimiento de normas, métodos, sistemas y procedimientos que deban seguir las distintas entidades con funciones de Policía Judicial para el desarrollo de sus objetivos, lo mismo que en la definición de competencias y responsabilidades que deban asignarse a las diferentes entidades que conforman el Consejo, en el propósito de aprovechar las ventajas comparativas de cada una de ellas y la eliminación de duplicidades en los sistemas.

Es adicionalmente el órgano dentro del cual deben solucionarse los problemas de coordinación que puedan surgir entre las entidades que lo integran.

Desde el punto de vista propiamente operativo, compete a la Dirección Nacional del Cuerpo Técnico de Investigación de la Fiscalía, en el nivel nacional, organizar, dirigir, controlar y ejecutar las funciones de policía

judicial de la Fiscalía y coordinar con los otros organismos que tienen funciones de policía judicial, definición de mecanismos operativos que racionalicen y eviten la duplicidad de esfuerzos, dentro de los lineamientos fijados por el Consejo de Policía Judicial.

La Dirección Nacional del Cuerpo Técnico de Investigación cuenta también en el nivel nacional con una División de Investigaciones bajo cuya coordinación se ejerce el desarrollo operativo de las tareas y en el nivel Regional y Seccional, con Directores Seccionales de Policía Judicial. Las entidades que cumplen funciones de policía judicial tienen, entre otras, las siguientes funciones:

- a) Dentro del ámbito de sus competencias, recibir las denuncias o querellas que se presenten y adelantar las diligencias preliminares.
- b) Adelantar con sujeción a las normas y el respeto por los derechos humanos, todas las actividades inherentes a la investigación de los hechos punibles que les correspondan.
- c) Realizar las investigaciones que las Unidades de Fiscalías les asignen.
- d) Solicitar a las Unidades de Fiscalía las órdenes de captura, allanamientos, interceptaciones de líneas telefónicas, registros de correspondencia y vigilancia electrónica, requeridas dentro de las investigaciones.
- e) Rendir informes, mediante certificación jurada a las unidades de Fiscalías.

Bajo este marco normativo es que la Fiscalía viene estudiando con algunas entidades públicas que ejercen funciones de control y vigilancia, la posibilidad de asignarles funciones de policía judicial a algunas de ellas, obviamente frente a los delitos que aparecen como de común ocurrencia en el sector y desde luego, conforme al ámbito de sus atribuciones. No se trata

de desviar de los organismos su función natural, sino de evitar duplicidad de esfuerzos en las tareas investigativas, para hacer valer plenamente en los procesos judiciales, todas las pruebas que se practican en la investigación administrativa.

Como quiera que las entidades de control, tienen personal especializado e idóneo en el desarrollo de investigaciones que por sus características requieren conocimientos especiales, se busca aprovechar ese recurso humano y además técnico, sin que ello implique una carga adicional distinta a la que se adelanta corrientemente.

Por citar un ejemplo, si la Superintendencia Bancaria encuentra en el desarrollo de su actividad que se ha podido cometer un delito de captación ilegal de dineros del público o se ha efectuado la actividad de intermediación financiera, sin la autorización requerida para el efecto, el conjunto probatorio que recaude el funcionario de la entidad, tendrá también carácter judicial.

ASPECTOS ORGANIZACIONALES

La Fiscalía cuenta con una estructura organizacional que se descentraliza hacia todo el territorio en cinco direcciones regionales y veintinueve seccionales, cada una de las cuales tiene el apoyo de las estructuras administrativa y de investigación correspondientes.

Entraña un profundo cambio, en el propósito de devolverle al aparato judicial su capacidad de investigación, particularmente en la lucha contra las organizaciones criminales del narcotráfico, el terrorismo, el secuestro y la extorsión, comportamientos estos considerados como los más desestabilizadores del orden institucional.

Lamentablemente, las organizaciones criminales cuentan con inmensos recursos financieros y técnicos que superan en mucho las posibilidades presupuestales de la Fiscalía. Ha estas organizaciones se les ha enfrentado

tradicionalmente con un esquema en el que defensa de las instituciones y de la legalidad corren por cuenta de funcionarios judiciales que llegan hasta el sacrificio sin contar con los mejores recursos en su lucha.

Debemos anteponer a las organizaciones criminales y a la delincuencia común una organización judicial capaz de proporcionar un medio eficaz y eficiente para investigar el delito y acusar a sus responsables. No bastan los instrumentos de un nuevo código procesal penal y de un nuevo ente judicial, es necesario aunar esfuerzos en materia de recursos presupuestales, técnicos de cooperación judicial y de capacitación, para obtener los resultados que nos proponemos. El concurso de la informática resulta vital en estas tareas, en favor de la calidad y eficiencia del sistema judicial. La sociedad en general y la comunidad internacional deben entender que quienes nos encontramos involucrados en esta lucha trabajamos en un objetivo común: La batalla contra la impunidad.

Requerimos un sistema de justicia sólido, libre de presiones indebidas o amenazas, de amedrantamientos y sobornos, de insidias y engaños, en el que la justicia prevalezca y quede claro que nadie, absolutamente nadie, puede colocarse por encima de la ley. Un sistema en el que a Fiscales y Jueces se les reconozca la estima social que corresponde a su alta investidura.

Dentro de este esquema de justicia, concebimos un nuevo Fiscal como una persona dotada de una cultura organizacional amplia en la que su habilidad, destreza y conocimientos le permitan delimitar su actuación a los justos términos que le corresponden y tomar decisiones sabias acertadas. Un individuo capaz de participar en los procesos de transformación y de cambio institucionales y, por sobretodo, un ciudadano dispuesto al servicio hasta el sacrificio, plétórico de patriotismo, honestidad y lealtad a toda prueba, y movido por el ideal de justicia que une a todos nuestros mártires inmolados en ya incontables trágicos sucesos.

La Fiscalía entiende su misión renovadora y por ello, participa activamente en la formulación de la política criminal del Estado y contribuye con sus informes al Ejecutivo al mantenimiento del orden público, tal como lo hizo en el pasado reciente cuando informó al Presidente de la República de los perjuicios que traería una errónea interpretación de las causales de libertad provisional en presencia de delitos de competencia de Jueces Regionales, en particular, en relación con procesos sobre narcotráfico. Así mismo, formuló algunas opiniones por conducto del Fiscal General sobre las alternativas jurídicas de solución al problema de secuestro y, al igual, considera en la actualidad similares alternativas para combatir la corrupción.

Hemos emprendido las tareas de modernización que los nuevos tiempos requieren, de tal suerte que en el futuro más próximo podamos contar con una entidad totalmente sistematizada en bien del servicio de la justicia.

Estimamos de suma importancia el proceso de capacitación de los nuevos Fiscales, en particular en las técnicas de la investigación criminal y criminalística, efecto para el cual venimos desarrollando un basto plan que se realice no solamente en Colombia sino también en el exterior.

Consideramos particularmente urgente la modernización de nuestros sistemas de investigación en escena del crimen, de los laboratorios de criminalística y fundamentalmente de seguridad a funcionarios.

En la lucha contra el narcotráfico la firme decisión de la entidad y de sus miembros de combatir este flajelo la ha llevado a ampliar los esquemas de la cooperación judicial internacional, mediante el envío de sus propios Fiscales a otros países, en procura de las evidencias contra los cabecillas del narcotráfico; a facilitar los instrumentos legales que permitan la incautación y decomiso de bienes destinados a la producción y procesamiento de sustancias estupefacientes, a combatir a las organizaciones dedicadas al comercio ilícito de precursores químicos, a pronunciarse sobre la presunta comisión de delitos en cárceles de alta seguridad como la Catedral de Envigado con un claro

sentido de independencia; a arremeter decididamente con la participación de otros organismos en operaciones orientadas a desarticular las bases financieras de las organizaciones criminales, a dar la lucha contra el enriquecimiento ilícito derivado del narcotráfico, a combatir a sus sicarios y testaferros y a participar, dentro del marco de sus funciones constitucionales y legales, en la política de sometimiento a la justicia que ha resurgido nuevamente en los últimos días con la entrega voluntaria de algunos delincuentes que se habían fugado en desarrollo de hechos acaecidos el pasado 21 y 22 de julio del año corriente.

Aún cuando legalmente solo entró a funcionar desde el 1o. de julio de 1992, con la antigua jurisdicción de Orden Público acumula ya (únicamente los procesos de competencia de los hoy Jueces Regionales entre los que se encuentran los delitos de narcotráfico), entre el 1o. de enero y el 30 de septiembre del presente año, 23169 autos de sustanciación, 8606 autos interlocutorios, 200 sentencias condenatorias, 40 absolutorias y 20 mixtas, para un total de 317 personas condenadas solamente en ese período y 110 absueltas.

Es en este foro en el que los hombres de la Fiscalía General de la Nación venimos a decir que estamos presentes y actuantes, que estamos concientes y caracterizados en nuestro papel, que todo aquel que pretenda colocarse por encima de la ley recibirá el castigo que merece y que cada vez que pretendan desviarnos de nuestro camino, incluso con la amenaza de la misma muerte, vendrá uno más, pletórico de entusiasmo a entregarlo todo de sí en bien de nuestra amada Colombia.

LA INTERACCION EN EL SECTOR FINANCIERO

Particularmente es la delincuencia organizada la que utiliza la estructura del sector financiero para cometer sus ilícitos, algunas veces incluso con la complicidad de los mismos miembros del sector. En algunas ocasiones por

ausencia de mecanismos de control (negligencia), en otras por el propósito de lucro fácil y rápido (dolo).

El sector financiero puede verse utilizado en la comisión de grandes fraudes económicos, estafas, falsedades documentales, receptaciones, y otra muy diversa gama de delitos económicos y contra el patrimonio individual.

Sin embargo, modernamente preocupa la utilización que se hace de algunas instituciones para el lavado de activos provenientes del narcotráfico, el ocultamiento, aseguramiento y receptación del producto de las actividades delincuenciales de la subversión y los llamados comúnmente fraudes financieros.

La actividad delictiva pretende legitimar ingresos producto de actividades ilícitas, evadir impuestos, efectuar pagos secretos, cambiar moneda ilegal por cheques garantizados por un banco, transformar moneda ilegal en objetos preciosos o coleccionables, invertir en el sector inmobiliario, etc. Así mismo, comprar empresas quebradas que generan ingresos brutos provenientes de ventas al contado, adquirir hoteles, agencias de cambio de moneda, restaurantes, empresas de máquinas expendedoras, etc.

En el proceso de atacar el lavado de activos y la financiación del terrorismo y la subversión, el Gobierno Nacional expidió el Decreto 1872 de noviembre 20 del presente año, en uso de las atribuciones propias de intervención en la actividad financiera y bursátil a que se refiere el artículo 50 transitorio de la Carta.

En efecto, se pretende evitar que a través de las operaciones que se realizan por las instituciones sometidas a la vigilancia de las Superintendencias Bancarias y de Valores, puedan canalizarse recursos o dineros que provengan de la ejecución de actividades delictivas.

Todos sabemos que el negocio financiero se ejecuta bajo el principio de buena fé, pero resulta innecesario que bajo el amparo de la costumbre de la reserva bancaria, se pueda crear un especie de protección para los criminales y ocultar información que sirva a las investigaciones.

La confianza del público en el sistema financiero es el motor que pone en funcionamiento toda su actividad. Es necesario entonces prevenir situaciones que puedan derivar en la pérdida de dicha confianza, por lo que dicho estatuto introduce obligaciones para las instituciones orientadas a evitar que sean utilizadas para el ocultamiento, manejo, inversión o aprovechamiento en cualquier forma de dinero u otros bienes provenientes de actividades delictivas, o para darles apariencia de legalidad a las mismas.

A éstos efectos, se obliga a las entidades vigiladas a diseñar y poner en práctica procedimientos específicos y designar funcionarios responsables de verificar el adecuado cumplimiento de ellos. Estos procedimientos se orientan en cuatro sentidos principales:

- a) Que la entidad conozca a su cliente en relación con su actividad económica.
- b) Que la entidad informe de manera inmediata y suficiente a la Fiscalía acerca de transacciones que por su poca habitualidad, volumen o forma de ejecución, puedan resultar sospechosas de que los clientes utilizan la entidad para invertir, manejar, ocultar o aprovechar recursos provenientes de actividades delictivas.

El esquema anterior entraña un sistema de intercomunicación con la Fiscalía que se basa en el hecho de que las entidades y sus funcionarios no pueden dar a conocer a las personas que hayan efectuado o intenten efectuar transacciones sospechosas, que han comunicado a la Fiscalía información sobre las mismas, y deberán guardar reserva sobre dicha información.

- c) La obligación de la entidad de suministrar información, cuando así lo soliciten los Directores Regionales o Seccionales de Fiscalías, directamente o por conducto de los demás organismos que ejercen funciones de Policía Judicial, para efectos de investigaciones sobre delitos de competencia de Jueces Regionales.
- d) La obligación de dejar constancia en formulario especial, de información relativa a transacciones en efectivo que realice en moneda legal o extranjera, cuyo valor sea igual o superior a \$ 7500.000, así como de las compras o ventas de divisas en efectivo, cuyo valor sea igual o superior a US 10.000 o su equivalente en otras monedas, con excepción de las operaciones entre entidades vigiladas. (Circular Externa No. 075 de diciembre 1o. de 1992).

Las instituciones financieras, en el desarrollo de éstos controles, deben adoptar medidas apropiadas que permitan determinar la existencia de transacciones múltiples pero que en realidad correspondan a una misma, efecto para el cual deben tomar en cuenta el conjunto de operaciones que se llevan a cabo en una misma oficina o en varias durante un mismo día y aquellas otras que sean capaces de acumularse con base en la aplicación de medios técnicos y operativos disponibles. (Circular 075 de 1992).

No pretende la Fiscalía llenarse de información respecto de la cual, en el momento no tiene siquiera capacidad de recibir. Se pretende que el banquero honesto que conoce su negocio, informe de lo que le parece irregular, por una parte, y por otra, que frente a solicitud de información por las personas indicadas, la institución le entregue rápidamente (cuestión que hoy no ocurre), sin poder oponer reserva alguna. Desde otro punto de vista, que con base en la información recibida y procesada por la Superbancaria, se conozca el movimiento de eventuales transacciones sospechosas, con base en las cuales, nuestros agentes adelanten las investigaciones pertinentes. Adicionalmente, que a través de un Comité, como nos lo propusiera el Señor Presidente de la Asociación Bancaria, en el que tenga asiento la Fiscalía, se efectúe por

las personas idóneas, un seguimiento al sector, de suerte tal que puedan detectarse mecanismos utilizados para fines delictivos.

Nos anima el mejor deseo de acertar y el convencimiento absoluto de que nadie, absolutamente nadie puede colocarse por encima de la ley y que quien la infrinja, recibirá el castigo que merece.

PAPEL DEL SECTOR FINANCIERO EN LA PREVENCIÓN Y CONTROL DEL LAVADO DE DINERO

*Jorge Gabriel Taboada Hoyos**

Por solicitud de la Asociación Bancaria y de Entidades Financieras de Colombia, me permito efectuar una breve síntesis de la presentación que al respecto del papel del sector financiero en la prevención y control del lavado de dinero, me correspondió realizar en el XI Seminario Nacional de Seguridad del Sector Financiero, que tuvo lugar en Villa de Leyva, del 3 al 5 de diciembre de 1992.

En primer lugar, mi intervención estuvo dirigida a explicar cómo el concepto de "lavado de dinero", entendido como un conjunto de maquinaciones dirigido a esconder el origen criminal de los fondos obtenidos por delincuentes mediante la comisión de delitos, ha hecho crisis.

En efecto, la figura clásica de "lavado de dinero" como actividad reprensible, evoca la época en la que las autoridades norteamericanas combatían a los

* Director General de Bancos e Instituciones Oficiales Especiales Superintendencia Bancaria.

llamados "raqueteros" y a los "gangsters" de Chicago, quienes obtenían efectivo mediante operaciones delincuenciales, que comprendían la venta de productos alcohólicos, entonces prohibidos, las casas de juego clandestinas y las casas de lenocinio, entre otros.

Entonces, el efectivo de la llamada "mafia de Chicago" era invertido en actividades económicas legales y respetables a través de mecanismos diseñados para el lavado de dinero. Por supuesto se requería que la participación de una institución financiera en tales mecanismos fuera intencional, es decir, que por lo menos algún empleado de esta interviniera a sabiendas en la respectiva operación de lavado; además, que la institución derivara alguna ganancia, por ejemplo, mediante las comisiones ordinarias que se cobraban por el manejo bancario de los fondos, para que se pudiera decir que la respectiva entidad se había involucrado en una operación de lavado de dinero, y que la misma tenía que ser investigada y sancionada por sus actos.

Hoy, en nuestro país la atención de las autoridades se dirige a cualquier manejo o transacción que involucre fondos obtenidos ilegalmente o dirigidos a un propósito ilegal, sea este el de esconder el producto económico de actividades criminales, o cualquier otro.

El propósito de las autoridades colombianas consiste en reducir al máximo la posibilidad de que los dineros obtenidos mediante actividades criminales, o dirigidos a las mismas, sean depositados o transferidos a través de instituciones financieras. Este es el marco conceptual que explica la expedición del Decreto 1872/92 del Gobierno Nacional, y la Circular 075 de 1992, de la Superintendencia Bancaria. Las normas a las cuales me refiero se encuentran divididas en dos partes:

La primera parte del Decreto 1872 establece para los bancos el deber de conocer a sus clientes, y el de avisar a las autoridades cuando la actividad económica de los mismos (que debe ser conocida por el banco) no parezca,

a juicio del banco, coherente con los balances o con las transacciones que los mismos registren.

Se establece además el deber de reportar a las autoridades cuando las transacciones de los usuarios de los bancos parezcan sospechosas.

La segunda parte del Decreto se refiere a los reportes de efectivo, los cuales, compilados, permitirán a las autoridades conocer el movimiento usual, los ciclos, y el volumen de las transacciones en efectivo dentro del país. Información que también podrá ser utilizada, en ciertos casos, para investigar cambios y tendencias en los patrones de comportamiento de las organizaciones delincuenciales.

Como podrá verse, el nivel de la responsabilidad que compete a las instituciones financieras es más elevado que el que les cabía bajo la concepción clásica del problema. De hecho, no es necesario que un banco o algún funcionario del mismo se encuentre involucrado en una operación de manejo de dinero ilícitamente obtenido, o siquiera que algún funcionario tenga motivos para sospechar de ciertas transacciones, para que el manejo de fondos ilícitos mediante la institución que los delincuentes decidan utilizar pueda acarrear sanciones a la misma.

Bastaría que se comprobara que el banco en cuestión no tomó las medidas necesarias para conocer al cliente, utilizado por los propietarios del dinero ilícitamente obtenido como testafarro, o que conociéndolo no diera oportuno aviso a las autoridades cuando la situación económica del mismo no explicara los movimientos o las transacciones registradas en sus cuentas con la institución.

El simple hecho de que los bancos no cumplan con el deber legal de conocer a sus clientes es, por si mismo, una infracción al Decreto 1872, independientemente de que dichos clientes estén o no involucrados en actividades ilegales.

Las normas citadas hacen ver que para las autoridades y para los banqueros, las operaciones pasivas involucran riesgos, al igual que lo hacen las operaciones activas, pero de diferente naturaleza.

Es necesario crear una conciencia en ese sentido, y disponer los mecanismos necesarios para manejar adecuadamente el riesgo que significa la parte pasiva de la operación bancaria, y que consiste en que mediante dicha operación pueden manejarse fondos ilícitamente obtenidos, con grave perjuicio para la sociedad.

La nueva Constitución Política de Colombia impone a las empresas, ahora de manera explícita, una función social, y además determina en particular que la actividad financiera es de interés público, lo cual en nuestro concepto significa nuevas prerrogativas, y nuevas responsabilidades.

LINEAMIENTO PARA UN CODIGO DE CONDUCTA DEL SECTOR FINANCIERO

*María Fernanda Guerrero Mateús**

Sin ir muy lejos hace unos años en los círculos bancarios del mundo, la práctica bancaria se caracterizaba por tres aspectos fundamentales: En primer lugar, "el dinero no tenía olor ni color" y "no se les exigía a los banqueros responsabilidad por la escogencia de sus clientes". En segundo lugar, los banqueros no tenían que ponerse en el trabajo de averiguar la moralidad de sus clientes ni la procedencia de sus dineros; y por último, el dinero en efectivo era la moneda universal de preferencia antes que el crédito. No sobra además agregar, que antes no existía la tecnología y hoy hablamos de dinero electrónico y de las operaciones de banca electrónica.

Ciertamente desde la década de los setentas, las reglas del juego cambiaron y con ellas el resurgimiento de lineamientos deontológicos, que deben guiar la actividad bancaria. Hoy por hoy el establecimiento de medidas como quieran que éstas se llamen, sean Recomendaciones o Códigos de Etica o Conducta, buscan imponer lo que deben ser o lo "conveniente" a fin de ordenar las relaciones entre distintos sujetos en el tráfico negocial. Efectivamente esto está sucediendo en el sector bancario, cuando no es un secreto para nadie que

* Abogada investigadora Asociación Bancaria y de Entidades Financieras de Colombia.

las instituciones financieras que lo componen pueden ser utilizadas sin saberlo, como intermediarios para las transferencias o el depósito de fondos originados en cualquier actividad criminal.

Basándonos en ese principio según el cual los negocios bancarios deben sustentarse en una relación de mutua confianza y absoluta honestidad para continuar manteniendo la solidez, la estabilidad y la credibilidad del sector bancario y financiero es prioritario el establecimiento de medidas de distinta índole que sirvan para prevenir, detectar y reprimir el lavado de dinero de dudosa procedencia.

Así las cosas, no obstante la importancia y complejidad que se advierte en el tema para ser tratado profundamente desde el punto de vista jurídico y económico, el objetivo principal de éste documento se circunscribe a mostrarles sólo algunos esquemas legales que regulan el blanqueo de capitales, reconocido de ante mano que es sólo a título ilustrativo. Se han escogido sólo aquellos que han sido susceptibles de recientes reformas y que además no han sido analizados por los estudiosos del tema. Por ello no se incluyeron las iniciativas legislativas de países tales como Reino Unido, Alemania, Estados Unidos, Islas Caimán, Suiza, Australia y Hong Kong.

INICIATIVAS, RECOMENDACIONES Y REGULACIONES PARA LA PREVENCIÓN Y REPRESIÓN DEL LAVADO DE DINERO ADOPTADAS POR ORGANISMOS INTERGUBERNAMENTALES

En la búsqueda de soluciones de carácter legal para afrontar el problema del lavado de dinero de proveniencia criminal, se han dado dos tendencias bien definidas a las cuales los países actualmente se están adhiriendo.

Una primera tendencia considera que el blanqueo de capitales debe combatirse principalmente con medidas de carácter penal y en el marco de la

cooperación internacional, entre autoridades judiciales y policiales. Esta concepción está desarrollada principalmente por dos cuerpos de normas, a saber:

- a) **La Convención de las Naciones Unidas** contra el tráfico de estupefacientes y sustancias sicotrópicas, aprobada en Viena el 19 de diciembre de 1988 (denominada Convención de Viena),
- b) **Convenio del Consejo de Europa** sobre el blanqueo, identificación, embargo y decomiso de los productos del ilícito, abierto a la firma el 8 de noviembre de 1990, en Estrasburgo.

La segunda tendencia corresponde a la concepción según la cual, la estrategia de lucha contra el blanqueo de capitales no debe limitarse exclusivamente al enfoque penal, sino también desde la perspectiva del sistema financiero; ya que este puede desempeñar una función sumamente eficaz. Las normas que desarrollan esta segunda opinión son las siguientes:

- a) **Recomendación del Consejo de Europa**, del 27 de junio de 1980.

En el plano de cooperación internacional esta recomendación constituye una de las primeras iniciativas en la lucha contra el blanqueo de capitales. Se concluyó en esa oportunidad¹ que "el sistema bancario puede desarrollar un rol preventivo extremadamente eficaz y que, al mismo tiempo, la cooperación de los bancos puede ser de auxilio, en la ejecución de tales actos criminosos, para la autoridad judicial y de policía". De ahí que en los años sucesivos el problema de la prevención del reciclaje de fondos de origen criminal a través del sistema financiero, centró toda la atención de los órganos legislativos, judiciales y de policía, y también de las autoridades de vigilancia bancaria de diversos países.

1. "Medidas contra la transferencia y la custodia de fondos de origen criminal" Recomendación N. R. (80) 10 adoptada por el Comité de Ministros del Consejo de Europa el 27 de junio de 1980.

- b) **Declaración de principios adoptada en Basilea,**¹ en diciembre de 1988, por el Comité de Regulaciones y Supervisión bancaria del Grupo de los Diez.

El propósito de la Declaración consiste básicamente en delinear algunas políticas y procedimientos fundamentales de los cuales los responsables de los bancos deberán asegurar su aplicación al interior de sus propias instituciones, para contribuir a la represión del reciclaje de fondos a través del sistema bancario nacional e internacional.

Se propone por lo tanto: fortalecer la **vigilancia bancaria**, adoptar medidas de **prevención** y prestar una **colaboración** eficiente con las autoridades judiciales y de policía.

Los **principios** contenidos en la Declaración se concretan en los siguientes puntos:

- **Identificación de la clientela** tanto para quienes poseen cuentas bancarias, como para quienes utilizan las cajillas de seguridad.
- **Conservación de documentos** para efectos probatorios.
- **Observancia de las leyes** y de rigurosos principios éticos concernientes a las operaciones financieras.
- **Colaboración con las autoridades judiciales y de policía** en cuanto al deber de informar, suministrar información, y de aplicar ciertas medidas al cliente cuando se presuma que éste efectúa operaciones derivadas de actividades ilícitas. Estas medidas son por ejemplo: el rechazo de proporcionar asistencia, la interrupción de las relaciones con

1. En 1988, el Bank of International Settlement de Basilea, Suiza, adoptó la regla de "conozca a su cliente".

el cliente y el cierre o congelamiento de las cuentas. El cancelamiento no es una medida preventiva que los bancos autónomamente puedan autorizar, son competentes únicamente las autoridades jurídicas y de policía.

- **Adhesión a la declaración** en la medida en que todos los bancos deberán adoptar formalmente políticas coherentes con los principios enunciados en la Declaración. Deberán asegurar la consecución de programas de formación para el personal del banco y la organización de controles internos.
- c) **Directiva del 23 de marzo de 1990** por la cual se incrimina el lavado de dinero e impone a los bancos de los países miembros la obligación de informar ciertas operaciones. Incluye el concepto de lavado de dinero a todos los fondos provenientes de delitos mayores y el terrorismo¹.
- d) **Directiva del Consejo 91\308\CEE²**, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales, expedida por la Comisión el 10 de junio de 1991.

Esta Directiva está dirigida fundamentalmente a prevenir que el sistema financiero sea utilizado para llevar a cabo operaciones de lavado de dinero, a fin de realizar plenamente el Mercado Unico Bancario para 1993. Países de la misma CEE como España, Bélgica, Luxemburgo, Reino Unido y Alemania ya adoptaron la Directiva y han procedido hacerla efectiva en su derecho interno, mediante la expedición de normas, reglamentos, y manuales instructivos. Así pues, la Directiva busca concretar los siguientes aspectos:

1. "Revista de derecho bancario y de la actividad financiera". No. 4. Ed. Depalma. Buenos Aires, julio-agosto de 1991, pág. 801.

2. Diario Oficial No. L 166/78.

- Tipificar como delito las operaciones de blanqueo de dinero del crimen organizado, en los doce países de CEE antes de enero de 1993.
- **Incluir dentro del concepto de crimen organizado** los delitos relacionados con narcotráfico, terrorismo y tráfico de armas.
- Imponer el deber de **identificar** tanto a los clientes habituales como a los ocasionales que realicen operaciones superiores a 15.000 ECUS (unos 2 millones de pesetas o 14 millones de pesos colombianos).
- **Imponer el deber de informar** de los empleados y directivos bancarios que descubran operaciones sospechosas de blanqueo de dinero, a través de la persona designada por su banco, a las autoridades responsables de la lucha contra el blanqueo de capitales, proporcionando a su vez toda la información que les sea requerida, sin que los bancos sean demandados por no respetar el secreto profesional.
- Se crea el "**Comité de Contacto**" o "**Comité**", cuyas funciones son:
 - Facilitar una aplicación armonizada de la Directiva.
 - Facilitar una concertación entre los Estados miembros, con las condiciones y obligaciones más rigurosas.
 - Aconsejar medidas complementarias o enmiendas a la Directiva
 - Examinar e incluir profesiones o categorías de empresas que también constituyan mecanismos de lavado de dinero
- Establecer los **procedimientos adecuados de control interno y de comunicación** y de **programas especiales de formación** a efecto de que los empleados conozcan y puedan detectar las operaciones de lavado y saber igualmente como proceder en esos casos. Estas medidas pueden ser más estrictas que las establecidas en la Directiva.

- **Conservar documentos** relacionados con la identificación y el registro de transacciones para fines probatorios. El término se ha establecido en cinco años, a partir del momento en que hayan finalizado las relaciones con el cliente; y, desde el momento que haya ejecutado la transacción.
 - **Colaborar con las autoridades responsables** con la lucha contra el lavado de dinero. La colaboración se concreta en los deberes de **informar oportunamente cuando se tenga conocimiento del hecho, facilitar información y no comunicar la sospecha al cliente afectado o a terceros.**
 - **Divulgar**, de buena fe, a las autoridades responsables lo que no constituirá **violación a las restricciones** impuestas al deber de informar.
 - Imponer a las entidades de crédito e instituciones financieras **el deber de abstenerse de ejecutar** transacciones, cuando estas sean sospechosas.
- e) **Recomendaciones del Grupo de Acción Financiera (GAFI)** sobre el blanqueo de capitales.

Emitidas por esta organización creada en julio de 1989 en la cumbre de París y en la que participan quince países, propugnan por que las medidas adoptadas a nivel nacional sobre el problema del blanqueo de capitales, deben estar acordes con las que emprendan otros países del área comunitaria.¹

1. Igualmente, la Federación Bancaria de la CE cuenta actualmente con un Grupo de Trabajo de Fraude, cuya misión es esencialmente estudiar las cuestiones relativas al lavado de capitales y otros aspectos del fraude internacional.

Su trabajo consiste principalmente en cambiar información de acuerdo a las reglamentaciones nacionales para así establecer nuevos tipos de fraude y los mecanismos de prevención. El Grupo estudia actualmente acciones concretas para que los bancos las lleven a cabo, de acuerdo con la Directiva del 10 de junio de 1991.

Las actividades del Grupo responden a reglas estrictas bajo un plan de confidencialidad de las informaciones.

f) **Recomendaciones de la Comisión Interamericana contra el abuso de drogas CICAD**, entidad de la Organización de los Estados Americanos OEA.

Tienen por objeto lograr que los países miembros adopten una legislación en materia de lucha contra el narcotráfico y el lavado de dinero. En términos generales busca concretar tres claros propósitos, a saber: incriminar el lavado de dinero en todo el continente; facilitar la identificación, embargo y decomiso de bienes; fortalecer la cooperación internacional en materia de investigación y procedimientos.

Con la aprobación del reglamento especial de la CICAD para impedir el lavado de dinero en las entidades financieras de 22 países, quedó sin piso el secreto bancario, bajo cuyo amparo se ocultaban los dineros provenientes del narcotráfico. Los aspectos más importantes del reglamento, son los siguientes:

- Sobre el **secreto bancario** consagra en su artículo 19, la estrategia que permitiría acabarlo. "Las disposiciones legales referentes al secreto o reserva bancaria no serán un impedimento para el cumplimiento del presente reglamento, cuando la información sea solicitada o compartida por un tribunal o por autoridades competentes, conforme a derecho".
- Dispone que una **orden judicial o sentencia firme**, que condene el decomiso de bienes, expedida por un tribunal competente de otro Estado con relación al tráfico ilícito de estupefacientes o delitos conexo, "podrá ser admitida como prueba de que los bienes, productos o instrumentos a que se refiere tal orden o sentencia, pudieran ser sujetos a decomiso conforme a derecho". Se aclara en el reglamento que por decomiso se entiende la privación con carácter definitivo de algún bien, por decisión de un tribunal o autoridad competente.

- En relación con los **deberes de las entidades financieras**, establece que éstas deberán mantener cuentas **nominativas**. "No pueden mantener cuentas anónimas ni cuentas que figuren bajo nombres ficticios o inexactos". Sobre identificación del cliente y conservación de la información, establece que las entidades deben identificar debidamente a sus clientes y conservar todos los antecedentes relacionados con una operación, así como mantener registros que permitan la reconstrucción de las transacciones financieras que superen determinado monto.
- El reglamento **tipifica los denominados "delitos de lavado"** y dispone que serán investigados, enjuiciados, fallados o sentenciados por el tribunal o la autoridad competente, independientemente de que el delito de tráfico ilícito o delitos conexos hayan ocurrido en otra jurisdicción territorial, sin perjuicio de la extradición, cuando proceda conforme al derecho.
- Exige el **reforzamiento de la policía financiera**. Para ello se deben crear enlaces de policía en los llamados "paraísos fiscales" e intensificar el trabajo de los escuadrones especializados de policía financiera principalmente en el centro de Europa, Japón, E.E.U.U. y las islas caribeñas.
- Se establece la obligación para bancos y entidades financieras de **comunicar** a las autoridades todas las transacciones que resulten sospechosas, por ser "complejas, insólitas y significativas y que no tengan un fundamento económico o legal evidente".¹
- Sobre la **entrega de información** el reglamento de la CICAD establece que un pedido de asistencia de la justicia de otro Estado, compromete al país que lo recibe a "suministrar originales o copias autenticadas de los documentos y registros, comprendidos los de instituciones financieras y entidades gubernamentales".

1. "Estrategia contra el narcolavado acabaría con el secreto bancario". En el Espectador del 13 de marzo de 1992, pág. 11-A.

- g) **Medidas contra el lavado de dinero en los Acuerdos sobre servicios financieros en el marco del Grupo Andino y el Grupo de los Tres, G-3.**

Una constante en los acuerdos entre los países andinos y especialmente en el grupo G-3, ha sido el propósito de impulsar la creación de un **Centro Regional Andino de Coordinación e Información para la Lucha Contra el Narcotráfico**, con el objeto de intercambiar información y coordinar acciones para que los esfuerzos contra el tráfico de drogas, que se adelantan al interior de cada país, sean más eficaces.

De esta manera, las medidas contra el lavado de dinero están dirigidas a prevenir las transferencias y legitimación de activos permanentes del tráfico de drogas, mediante el establecimiento de controles preventivos administrativos y tributarios a nivel de instituciones financieras, a fin de llevar a cabo un seguimiento de capitales de dudosa procedencia.¹

INICIATIVAS DE DERECHO INTERNO

- a) **Mecanismos técnicos y jurídicos adelantados por la Asociación Española de Banca Privada AEB.**

De ese proceso de lucha contra el blanqueo de dinero, en España los bancos asociados a la AEB no solamente cuentan con las normas vinculantes de actuación y desarrollo de la **Declaración de Basilea**, suscritas en 1990, sino que además llevan a cabo reuniones de alto nivel en las que participan representantes de los bancos y cajas de ahorro, el Delegado del Gobierno para

1. Se consultaron los siguientes documentos del Acuerdo de Cartagena: Declaración de Galápagos: Compromiso Andino de Paz, Seguridad y Cooperación, Ecuador, 16 y 17 de diciembre de 1989; Acta de Caracas, mayo 20 de 1991; el documento emitido en la reunión de Ciudad de México del 22 de noviembre de 1990 (G-3), y La Declaración de los Presidentes de Colombia, México y Venezuela en Guadalajara, del 17 de julio de 1991.

el plan nacional sobre drogas, el fiscal antidroga, y representantes del Ministerio del Interior y del Banco de España y la CECA. Estas reuniones se han revelado de gran utilidad para armonizar criterios.

Para cumplir con los propósitos enunciados la AEB, a través de la Secretaria General, ha adoptado las siguientes medidas:

- **Circular número 420**, del 17 de julio de 1990 mediante la cual el Comité Ejecutivo de la AEB da a conocer a los bancos asociados las normas para la prevención del blanqueo de dinero de origen criminal en desarrollo y aplicación de la Declaración de Basilea.
- Poner en conocimiento de los bancos una **lista**, elaborada por un grupo de expertos de bancos españoles, que selecciona e identifica una serie de operaciones bancarias consideradas de una mayor atención; que han sido utilizadas frecuentemente por los delincuentes para blanquear dinero a través del sistema bancario. La lista no pretende ser exhaustiva ya que ésta es variada y se enriquece continuamente. Esta lista corresponde a los que se ha denominado **Perfiles de Operaciones para Análisis**.
- Ampliando el esquema anterior la AEB difundió igualmente entre los bancos, una lista elaborada por un grupo de trabajo de la Federación Bancaria de la Comunidad Europea,¹ que enuncia los ejemplos de **operaciones sospechosas** que sin duda pueden ayudar en la lucha contra la utilización del sistema financiero en blanqueo de dinero. Dichos ejemplos no tienen carácter limitativo ni pretenden agotar exhaustivamente todo el casuismo que pueda existir en tan complejo y delicado asunto.

1. Ha sido notable el esfuerzo realizado por la Federación para afrontar todo el esquema del Mercado Unico Bancario. En ese esfuerzo, tanto en el Consejo como el Comité Central y en los grupos de trabajo de la AEB, han examinado conjuntamente las normas comunitarias generales, entre las que se cuentan las relacionadas a la prevención del blanqueo de capitales. (En las Memorias 1991. AEB, pág. 10).

- Se elaboró y solicitó a los bancos el diligenciamiento del **cuestionario sobre las normas para la prevención del blanqueo de dinero de origen criminal**. El cuestionario fue enviado a todos los bancos asociados en noviembre de 1990. La gran mayoría de los bancos lo respondieron oportunamente y los datos obtenidos han sido de enorme utilidad para la Asociación, para afirmar las relaciones con las autoridades encargadas de la represión de la actividad criminal.

Se podría decir que desde esa fecha los bancos han avanzado significativamente en la implantación de medidas encaminadas a evitar ser utilizados, sin saberlo, como vehículos para el blanqueo de capitales procedente del narcotráfico. Por ello, la Asociación Española de Banca Privada solicitó que los bancos diligenciaran el mismo cuestionario con los datos referidos a los sucedido durante todo el año 1991.

Las respuestas al cuestionario tendrán un carácter **estrictamente confidencial**, por ello cada formulario va identificado con un número de referencia, para efecto del régimen interno.

Igualmente la AEB copatrocinó en junio del año pasado un **curso de especialización** en la investigación de fondos procedentes del tráfico ilegal de drogas, como una forma de llevar a cabo una actualización para bancos y altos funcionarios.¹

b) **Labores realizadas por la Asociación Bancaria Italiana-**

Italia es uno de los países donde mayor cantidad de leyes se han expedido para luchar contra el crimen organizado. Bajo este término se encuentra no solamente el lavado o reciclaje de dinero sino también mafia, terrorismo,

1. Sobre este aporte en materia de capacitación, se refiere el documento de la AEB que contiene la Memoria de 1991, publicado como informe de gestión en su pág. 9

secuestro, chantaje y evasión fiscal. El "arsenal" técnico y jurídico contra el blanqueo de capitales comienza con la consagración en el **artículo 648** del código penal italiano de sanciones para castigar el blanqueo de capitales, en los casos de robo, chantaje y secuestros.¹

Las normas más importantes que se expidieron entre 1979 y 1990 fueron las siguientes: el **Decreto-ley 625** que prevé la obligación de registrar todas las transacciones financieras que superen los 20 millones de liras, realizadas a través de la administración, los bancos y el correo; la **ley antimafia** de septiembre de 1982 y el **Decreto-ley 272** de 1987; la **ley 55 de 1990** y el **Decreto 91** del mismo año que contienen disposiciones para la prevención de la delincuencia de tipo mafioso, y otras manifestaciones de la peligrosidad social.

En cuanto la normatividad para el control de las operaciones efectuadas con medios de pago y para contrarrestar el fenómeno del reciclaje de fondos de proveniencia ilícita, se encuentra la **Ley 197 de 1991**, mediante la cual el legislador nacional introdujo las obligaciones de registro y de señalización, a cargo de los entes crediticios y financieros. Se modificaron así las leyes del 6 de febrero de 1980 y la del 19 de marzo de 1990.

La mencionada ley impone **limitaciones al uso del dinero y de los títulos al portador**, estableciendo que la transferencia de tales sumas o de tales títulos, de un importe superior a los 20 millones de liras debe ser efectuado a través de los intermediarios habilitados (entes crediticios, oficinas de la administración pública y postal, compañías de seguros, agentes de cambios, sociedades de intermediación mobiliaria, fondos comunes de inversión, etc), o a través de otros medios previstos expresamente.

1. Las normas son el 648 (Ricettazione) y el 648 bis (sostituzione di denaro o valori provenienti da rapina aggravata, estorsione aggravata o sequestro di persona a scopo di estorsione). ("I Codice penale e di procedura penale e le leggi complementari". Casa Editrice la Tribuna-Piacenza 1998, pág. 228).

Igualmente se ha introducido una disposición que establece la obligación, para los intermediarios habilitados y para funcionarios públicos, de **notificar al Ministerio del Tesoro de las infracciones de las cuales tengan noticias en el ejercicio de sus funciones**, estableciendo sanciones administrativas pecuniarias por su omisión.

De otra parte, se ha previsto por la ley en mención el establecimiento de un **archivo centralizado** constituido y administrado con sistemas informáticos de cada intermediario financiero. Se instituye la obligación, para los representantes legales de los entes crediticios y para otros intermediarios financieros, de señalar cada operación efectuada de cualquier suma que por su entidad o naturaleza induzca a creer que el dinero, los bienes y la utilidad objeto de la operación misma provengan de uno de los delitos a los que se refiere el artículo 648 del C.P. (hurto agravado, extorsión agravado, secuestro de personas con fines de extorsión, delitos concernientes a la producción y el tráfico de estupefacientes o sustancias sicotrópicas).

Otras normas posteriores han sido el **Decreto-ley número 143 del 3 de mayo de 1991**, que consagra disposiciones urgentes para limitar el uso del dinero y de los títulos al portador en las transacciones y prevenir la utilización del sistema financiero con fines de reciclaje. En el establecimiento de medidas contra el lavado de dinero, ha sido notable la participación de la **Asociación Bancaria Italiana** y de la **Banca de Italia**.

En los primeros meses de 1990, la Asociación expidió a sus asociados dos circulares muy importantes: De un lado se encuentra la **Circular número 44** que contiene las medidas urgentes para la coordinación de la lucha contra la delincuencia de tipo mafioso, establecidas en la Ley número 55 del 19 de marzo de 1990; del otro está la **Circular número 29** que contiene los comentarios sobre el Decreto del 3 de mayo de 1990 del Ministerio del Tesoro, relativos con el ámbito de aplicabilidad de la norma (control de las operaciones y operaciones fraccionadas), la identificación de los sujetos que

intervienen (modalidad de registro y obligaciones de la clientela) y, los registros y escrituras para la anotación de los datos.

Igualmente La Presidencia de la ABI con el pleno convencimiento de la importancia del asunto para el sistema bancario, promovió la firma del **Acuerdo Interbancario sobre el tema de la identificación de la clientela**. Mediante este acuerdo los establecimientos de crédito se comprometen a no efectuar operaciones de sumas superiores a 10 millones de liras si no son personas conocidas o están en grado de hacerse identificar.¹

Este acuerdo representa la respuesta del sistema bancario italiano a las indicaciones contenidas en la "**Declaración de Principios**" del Comité de Basilea para las reglamentaciones bancarias y las prácticas de vigilancia, en la que se solicita a los entes crediticios atenerse a elevados principios éticos en el desenvolvimiento de la actividad bancaria y de proceder a identificar la clientela, la conformidad de las operaciones a las leyes nacionales y de otros países, y a la cooperación con las autoridades judiciales.

Los establecimientos de crédito italianos con el acuerdo en comento (que entra en los detalles de cada una de las operaciones, estableciendo un cierto casuismo, y también para fines de racionalizar y establecer estándares en la praxis de identificación) se comprometen:

- No efectuar operaciones por sumas no inferiores a 10 millones de liras sino con personas que ya conozcan o estén en grado de identificarse.
- No abrir depósitos de ahorro al portador, independientemente de la suma depositada o retirada, sin proceder a la identificación de la persona que efectúa la operación.

1. En Serie Informazioni - Circulare No. 29 de la Associazione Bancaria Italiana, Roma 9 maggio 1990, pág. 1.

- Conservar la documentación contable de modo tal que siempre sea posible reconstruir la particular operación.

El artículo 13 de la Ley del 6 de febrero de 1980, número 15 (sustituido por el artículo 2o. de la ley No. 197 del 5 de julio de 1991) obliga en cambio a identificar todos los sujetos que llevan a cabo operaciones (de transmisión o movimientos de medios de pago indicados en el Decreto del Ministro del Tesoro del 19 de Diciembre de 1991 es decir, en dinero en efectivo, con varios tipos de cheques y pagos bancarios y postales y órdenes de acreditar y de pagar) de sumas superiores a 20 millones de liras anotando los datos en un registro; de análogo cumplimiento antes del 1o. de junio de 1992.

En relación con esto aparece evidente cómo el ámbito de aplicación del acuerdo ha estado en parte absorbido por aquel del artículo 2o. de la ley No. 197 de 1991. También se hace relevante el cumplimiento del acuerdo mismo en cuanto a reconstruir las operaciones de sumas superiores a 10 millones de liras.¹

Por último, la **BANCA DE ITALIA** anunció que va a dar a conocer su "**decálogo antireciclaje**", que fue elaborado por un grupo mixto compuesto por la oficina italiana de cambios, el organismos de vigilancia y las fuerzas del orden. Las reglas allí contenidas definen el perfil de la red de protección para bloquear una operación en el momento en que se abra una cuenta sospechosa. El documento contendrá precisas indicaciones a las cuales deben atenderse para impedir la apertura de cuentas y de depósitos sospechosos, sobre todo aquellas que buscan reciclar el dinero derivado de actividades ilícitas vinculadas con el tráfico de droga.²

1. Comentarios de Asociación Bancaria Italiana, octubre 25 de 1992.

2. "Decalogo Bankitalia contra riciclaggio". En corriere della Sera Giovedì 2 aprile 1992, pág. 23.

Así mismo este año se creó, mediante la ley No 413 del Ministerio de las Finanzas, el **archivo electrónico antievasión y reciclaje** que tendrá por objetivo, revelar toda la información sobre cuentas corrientes bancarias que superen los 20 millones de liras. No obstante la utilidad que esta base de datos puede proporcionar, existen fuertes críticas centradas fundamentalmente en el hecho de que con esta medida se declara absolutamente la caída del **secreto bancario** y de otro lado no se tutela la **libertad y privacidad de los ahorradores**. Aunque se sostiene que la creación de esta base de datos es necesaria para luchar contra el crimen organizado, el reciclaje de dinero y la evasión fiscal, deben existir condiciones más precisas de reserva y de acceso y la solemne seguridad de que cualquier uso impropio de la información será impedido. La medida de "fichar" las cuentas corrientes bancarias debe provenir de una **claridad absoluta** y en un cuadro de certeza legislativa detallada. Se califica esta base de datos como una verdadera "**spia elettronica**" en favor de claros intereses públicos.¹

c) **Labores realizadas por la Asociación de Bancos Franceses.**

Los criminales que quieren enriquecerse impunemente mediante los "tráficos" financieros encuentran en el derecho positivo francés normas que reprimen y castigan severamente este tipo de conductas.

De otra parte se debe recalcar que estos problemas no pueden ser indiferentes para los auditores internos de los bancos ni para otros sectores de la economía. El sector bancario en general debe estar al corriente de las medidas tomadas por el legislador que ha querido dar a la policía y a los bancos medios para luchar eficazmente contra el flajelo de la droga.

La lucha contra la droga ha sido desde hace muchos años un objetivo prioritario de los poderes públicos en los países desarrollados. Se toma en

1. "Fisco in banca, subito guerra" e "Quell'occhio inquietante". En Corriere della Sera, Giovedì 2 aprile 1992, pág. 1 e 23.

consideración todos los factores de propagación de la plaga en acciones que sustentan tanto la oferta como la demanda de estupefaciente. La amplitud del problema y el poco éxito de la represión criminal directa, condujeron a emprender el combate con aquellos que ayudan en las operaciones financieras destinadas a la colocación de capitales de proveniencia ilícita. Este es sin duda, el sector esencial y obligatorio para las actividades criminales.¹

A este respecto el legislador francés ya ha dispuesto de normas adecuadas para crear el delito de blanqueo de capitales y de transferencias internacionales de fondos que se originan en el tráfico de droga. La experiencia, sin embargo, muestra que estas disposiciones no tendrán plena eficacia sin la colaboración activa de las entidades financieras y de manera muy general con todas las autoridades o profesionales que controlan el manejo de capitales.

Desde 1970 se ha reprimido penalmente el tráfico de estupefacientes en Francia. Mediante la **Ley del 31 de diciembre** de ese año: el transporte, porte, oferta, cesión, adquisición, empleo o el cultivo de estupefacientes se sanciona severamente. Lo mismo sucede con la importación, producción, fabricación o exportación ilícita de esas sustancias o plantas.

Solo recientemente la legislación francesa consagra las consecuencias financieras del tráfico y especialmente a raíz de la expedición de la **Ley del 31 de diciembre de 1987**. Esta ley llevó a que se modificarán dos artículos de el **Código de Salud Pública y del Código Aduanero**.

La primera modificación define el lavado de dinero "como la acción que facilita o que trata de facilitar la justificación falsa del origen de los bienes del traficante, o que aporta la ayuda a toda operación de colocación, simulación o conversión del producto de las infracciones". Se indica igualmente que este tipo de delito debe ser cometido con conocimiento de causa.

1. Christian LAJOIE, "El lavado de dinero y la ley francesa". Responsable de la verificación, en la inspección general del Banco Nacional Popular.

Las penas se establecieron en dos a diez años de prisión y eventualmente multas de 5.000 a 50.000 francos.

La segunda modificación consagra el hecho que proceda por exportación, importación, transferencia o compensación de toda operación financiera entre Francia y el exterior sobre fondos que provienen, directa o indirectamente, de una infracción a la legislación sobre estupefacientes.

El conjunto de normas ya establecidas ha implicado un reforzamiento progresivo de los mecanismos de investigación tanto de la aduana como de la policía. Los esfuerzos han sido de coordinación y especialización. De esta manera se previó crear simultáneamente dos organismos que persiguieran el lavado de dinero, sin que se limitaran exclusivamente al producto del tráfico de drogas. Estos organismos son: la **Oficina Central de la Represión de la Gran Delincuencia Financiera (O.C.R.G.D.F.)** y el **Organo del Tratamiento de la Información y de la Acción contra los Circuitos Financieros (TRACFIN)**.

El primero coordina o interviene en casos de infracciones de carácter económico, comercial y financiero relacionadas con la criminalidad profesional u organizada, en especial aquellas que tienen que ver con el banditismo, el terrorismo y el tráfico de drogas.

El segundo trata la información y coordina la acción del Ministerio de las Finanzas, en particular los servicios aduaneros en materia de circuitos financieros clandestinos o de blanqueo de dinero.

d) **Estrategias montadas por el Gobierno Canadiense-**

En Canadá el sistema bancario por ejemplo creó la que ellos denominaron **Fuerza de tarea de lavado de dinero** compuesto por directores de seguridad de los principales bancos canadienses. Se examinó el problema a nivel local, regional, nacional e internacional. Este grupo cuenta con la colaboración de

la **Policía Montada Real Canadiense**¹ y también de los representantes de las autoridades ejecutivas de la ley provinciales y municipales.

Los bancos canadienses desarrollaron políticas y procedimientos internos a través de sus sucursales nacionales e internacionales.

También se desarrollaron instrumentos de **capacitación**, se diseñaron procedimientos de informes, así como **intercambio de información, documentación y experiencias** sobre lavado de dinero. Los bancos han adoptado un programa interno basado sobre la regla de "**conozca su cliente**" la buena práctica bancaria.

Todos los bancos han establecido **formularios de informes internos** para grandes transacciones en efectivo poco usuales y sospechosas. Los cajeros deben diligenciarlas para transacciones que excedan de C\$10.000.(dólares canadienses). El cliente debe decir de donde procede el dinero y debe firmar el formulario. También hay un **informe de transacciones a la policía montada**.

Funcionamiento de la comunicación de la filosofía anti-lavado:

- Se comunica a los banqueros a través de procedimientos escritos entregados a todos los empleados en las sucursales, especialmente a los que atienden por ventanillas. Estos deben estudiarlos y firmar su recibo.

- A través de **capacitación** (videos)

1. La colaboración se manifiesta cuando reciben por parte de los departamentos de seguridad de los bancos, los informes de las transacciones sospechosas. El promedio de operaciones sospechosas reportadas por los Bancos en 1989 fue de 100 mensuales y en 1990 de 75. (Michael E.P. Ballard. "El enfoque de la Banca Canadienses en la lucha contra el lavado de dinero". Asociación Bancaria Canadienses. Toronto, 1991).

Existen estrechas relaciones con el poder judicial y con el gobierno (Comité Ministerial) y también con el órgano de supervisión bancaria (Superintendencia de instituciones financieras).

La ley sobre lavado de dinero es en Canadá, solamente un fundamento para el enfoque del problema. Por ello las políticas y procedimientos deben complementarla.¹

e) **Mecanismos jurídicos de dos países Latinoamericanos**

En el contexto latinoamericano, por ejemplo, **Panamá** cuenta con la ley 23 de diciembre de 1986. Mediante esta ley se tipifica el lavado de dinero como delito. Se castiga por ejemplo: proporcionar información falsa para la apertura de cuentas o la realización de transacciones y, también el que se vale de su profesión, función u oficio para autorizar o permitir que se comentan delitos de esta naturaleza. Se castiga al encubridor y a estas personas con dos a cinco años de prisión.²

Igualmente la **Asociación Bancaria de Panamá** desde 1984 ha establecido medidas de lucha contra el crimen organizado. Estas disposiciones concuerdan con los principios propugnados por el Consejo de Europa, la Convención de Viena y con el Acuerdo de Basilea.

En la legislación **Argentina**, se prevé la ley 23.737 del 21 de septiembre de 1989, destinada a regular y sancionar el tráfico de estupefacientes. Sancionan el lavado de dinero producto del narcotráfico y se establecen normas de decomiso de los bienes y ganancias derivados de los delitos previstos en la ley. Las disposiciones contenidas en esta ley son consideradas de amplio

1. Michael E. P. Ballard. "El enfoque de la banca canadiense en la lucha contra el lavado de dinero". Asociación Bancaria del Canadá. Toronto, Ontario, 1991.

2. "Concepto de lavado de dinero según la ley Panameña". En revista ABP Informa, Centro Financiero julio-agosto de 1991, pág. 13.

alcance ya que, por ejemplo estas normas, se extienden no sólo al sector financiero sino también a otras profesiones y actividades en cuyo ejercicio se pueda participar en un acto de narcolavado. Aparece claro también que esa extensión de las normas citadas obliga en la práctica a cumplir un deber de diligencia, para establecer la **identidad** y características de la persona que celebra operaciones con las entidades bancarias.¹

Por su parte la **Asociación de Bancos Argentinos** ya cuenta con la guía de recomendaciones para los bancos asociados para prevenir la realización de operaciones de lavado de dinero proveniente del narcotráfico. Los principios que propugna son coherentes con los contenidos en la Declaración de principios de Basilea, vale decir, identificación del cliente, archivo y conservación de documentación, suministro de información, denegación de asistencia e información y entrenamiento de personal.

Finalmente como un ejemplo adicional, pero del área de Centroamérica, el Congreso de **Guatemala** aprobó una nueva y drástica ley que establece la pena de muerte y condenas mayores para quienes sean hallados culpables de participar en actividades de tráfico de drogas. Así mismo la mencionada ley permite combatir el lavado de dinero y faculta a los tribunales y al Ministerio Público para recabar del sistema bancario las cuentas de los sospechosos.²

f) **Posibilidad de instrumentos jurídicos contra el lavado de dinero en Colombia-**

Hace pocos meses, la Asociación Bancaria de Colombia en el proceso de investigación sobre el tema consultó a la **Superintendencia de Control de Cambios**, sobre las formas detectadas y comúnmente utilizadas para llevar

1. Asociación de Bancos Argentinos (ADEBA). "El lavado de dinero proveniente del narcotráfico y la preservación de los sistemas financieros". En Rev. de Derecho Bancario y de la actividad financiera. Ed. Depalma, Buenos Aires, año 1, julio-agosto de 1991, pág. 832.

2. "Pena de muerte a narcos en Guatemala". En el Espectador del 25 de septiembre de 1992.

a cabo el lavado de dinero, utilizando el sistema bancario colombiano. De esta manera se pudo concretar cuatro variantes, a saber:

- **El reintegro por exportaciones o exportaciones ficticias** en la que los Bancos se sirven de intermediarios para que el exportador pueda traer sus divisas fruto de la exportación. Los problemas se han presentado porque existe el aforo documental lo que no permite la posibilidad de verificación física de la mercancía. Se presentan, entonces, casos de una simulación de una exportación y anomalías (sobrefacturación) en la exportación llevada a cabo legalmente. Los factores motivacionales para quienes incurrir en las infracciones son: la devolución del IVA y el reembolso de los Cert y evitar el impuesto de retención en la fuente por venta de divisas por servicios y transferencias. Tanto las personas jurídicas (generalmente sociedades de papel) como las personas naturales pueden ser sujetos activos de la infracción. De ahí que se recomienda verificar la identificación, nombre, referencias y existencia de los que eventualmente pueden efectuar lavado de dinero.¹
- **Ingresos personales** que hacen parte de las llamadas Divisas de libre disposición. No obstante los ítems de ingresos por venta de bienes y servicios al turista y las transferencias y donaciones pueden servir de disfraz para los dineros provenientes de actividades ilícitas. El comportamiento consiste en fraccionar grandes sumas para declararlas en distintas épocas.
- **Compra de divisas por ventanilla.** Esta variante puede explicarse a través de un caso ya detectado en una casa de cambio que contratava extranjeros a quienes se les pagaba una comisión (1%), para que vendieran divisas a los bancos y Corporaciones Financieras de manera fraccionada. Esta modalidad fue utilizada pensando en que los extran-

1. Las autoridades de impuestos, Aduana, Banco República, y la Superintendencia Bancaria han denunciado el aumento del lavado de dinero mediante exportaciones ficticias. Esto afecta directamente las entidades financieras, que de acuerdo con la resolución 57 son las encargadas del mercado cambiario.

jeros que quieren cambiar moneda lo pueden hacer sin ningún tipo de restricciones. Es aconsejable que los bancos sepan que esta modalidad existe y estar atentos cuando reiteradamente un extranjero cambie dólares.

- **Camuflar la inversión extranjera** (posiblemente se utilice en un futuro próximo). Es el caso de un Colombiano que constituya una sociedad extranjera para invertir en Colombia y de esta manera traer divisas y lavar dinero.

De la consulta se logró establecer que lo más prudente para las entidades del sector bancario es tratar al máximo de establecer pautas para identificar al cliente y lograr toda la certeza sobre la existencia de sociedades. Igualmente es recomendable contar con mecanismos de información sistematizada para lograr determinar una mayor credibilidad sobre quién es el cliente y si la sociedad es real o de papel.

En materia legislativa el Gobierno del Presidente Gaviria, sometió al Congreso de la República, en febrero de este año, el proyecto de ley mediante el cual Colombia se adhiere a la **Convención de Viena** y recientemente, en los términos establecidos en la conferencia cumbre de San Antonio, Texas, el **Acuerdo para intercambiar información financiera** para los casos que tengan que ver con el lavado de dinero de proveniencia ilícita. De otra parte, no sobrá recordar que la Junta Directiva del Banco de la República en el transcurso de éste año ha expedido Resoluciones especialmente para las casas de cambio que de alguna manera indican procedimientos para prevenir el lavado de dinero.¹

A pesar de los beneficios que su aprobación pueda reportar para el derecho positivo colombiano, quedarían por regular los aspectos que de manera

1. El Proyecto de Ley No. 24 del Senado. El Acuerdo Estados Unidos Colombia no fue aprobado en la legislatura pasada.

directa tienen que ver con el sector financiero. Por ello, tanto la ASOCIACION BANCARIA Y DE ENTIDADES FINANCIERAS DE COLOMBIA como algunos bancos ya están en la tarea de elaborar **Códigos de Conducta** que contienen las pautas mínimas coherentes por ejemplo con las iniciativas propuestas en Basilea y en la CEE, a las cuales las entidades deben someterse para no ser utilizadas sin saberlo para llevar a cabo conductas de lavado de dinero.¹ En este propósito están empeñados igualmente, el Gobierno, las entidades de vigilancia y control y los máximos organismos de seguridad del Estado.

CONCLUSIONES

De la comparación entre los distintos textos legales, se concluye lo siguiente:

1. Las medidas legales que conducen a prevenir el lavado de dinero giran alrededor de la identificación del cliente, **conservación de documentos, cumplimiento de principios éticos y capacitación**. Son esencialmente normas vinculantes.
2. No abarcan únicamente la procedencia del lavado por razones de narcotráfico, sino también de **cualquier conducta de la criminalidad organizada, terrorismo y tráfico de armas**. Las normas se extienden igualmente a **cualquier empresa o profesión susceptible de ser utilizada en el ilícito**.²

1. Sobre el particular algunos bancos colombianos, por instrucciones de la Superintendencia Bancaria, ya expidieron sus códigos de ética para prevenir que fueran utilizados para el lavado de dinero. Es el caso del Banco Industrial Colombiano, que expidió el código de ética en agosto de 1991, el Banco Colombo-americano, en junio de 1991, el Banco Ganadero, Panamá entre otros.

2. A los establecimientos de comercio, especialmente joyerías, venta de automóviles, galerías de arte y otros establecimientos donde el cliente al adquirir la mercancía de un costo muy alto paga en dinero en efectivo. Igualmente las compañías exportadoras e importadoras de mercancías pueden ser centros de lavado de dinero debido a que los precios de los productos raramente se inspeccionan.

3. Se pueden identificar y calificar conductas que induzcan a pensar cuales operaciones son sospechosas. Es por ello que a partir de la práctica bancaria, se puede elaborar una lista de ejemplos para ser difundida en todo el sector bancario. No es nunca una lista exhaustiva, debe complementarse con los hechos que se vayan conociendo.
4. Los **Códigos de Conducta** vienen siempre acompañados por unos **procedimientos** que son de hecho la forma de poner en práctica los principios éticos. En estos procedimientos se prevé por ejemplo los **formatos para recepcionar los datos que conciernen al cliente** a efecto que lo identifiquen inequívocamente. Igualmente, cuestionarios, para recepcionar, controlar y establecer estadísticas con respecto a las conductas delictivas de lavado de dinero.
5. La principal propuesta es lograr una **reforma al Código Penal**, a fin de que se tipifique como hecho punible el lavado de dinero.
6. En razón al actual perfil de quienes se dedican a la labor de la seguridad bancaria, es prioritario establecer pautas y nuevas exigencias para que sean cumplidas por estas personas con el propósito de renovar los viejos conceptos de la seguridad exclusivamente física, por aquellos más avanzados de **seguridad integral**.
7. Sin duda los efectos jurídicos de las normas comentadas dejan entrever problemas que ya se están presentando en algunos países. Son ellos, la **caída de la noción de secreto bancario** y las consiguientes manifestaciones como lo están haciendo los otros países de **violación de los datos personales** de los clientes. Sin embargo, esa dicotomía entre la protección de datos personales y los derechos fundamentales ante la criminalidad organizada, aunque en algunas legislaciones ya ha sido resuelta, lo cierto es que encuentra una loable justificación en un interés general.

8. Dependiendo del nivel de avance tecnológico, algunos países cuentan con **herramientas tecnológicas importantes** para luchar eficazmente contra el blanqueo de capitales. Se prevé medidas tanto para las operaciones documentales como para las electrónicas.
9. Las medidas establecidas por un "código de conducta" no deben ser óbice para que las entidades mutuo propio, establezcan algunas **medidas más estrictas y particulares**.
10. La razón de la similitud de las normas comentadas está en las iniciativas de **integración** tanto regional como internacional, como es el caso de la CEE. La idea es lograr una armonización mediante una concertación con los países miembros para aplicar las medidas.
11. Un común denominador en las legislaciones analizadas es también de apoyar las políticas contra lavado mediante el establecimiento de **bancos de datos**. La eficacia de las medidas está en poseer excelentes sistemas de información.
12. Como en el fraude electrónico, en los delitos de lavado de dinero también existe la posibilidad de que los motivos de comisión del delito se generen por **corrupción e infidelidad de los mismos funcionarios que sirven a la entidades bancarias**. Por ello, deben existir exigentes mecanismos de selección del personal.
13. Por ser el blanqueo de capitales una infracción calificada como delito masa, de cuello blanco, de carácter económico y con capacidad de traspasar fronteras; las políticas y procedimientos establecidos al interior de cada país, no son suficientes sino se tienen en cuenta en un contexto de la Comunidad Internacional.
14. Las formas de lavado, las operaciones bancarias utilizadas y la misma definición de lavado de dinero no han sido precisadas con exactitud en el ámbito jurídico. En la práctica los Código de Conducta y los procedimientos para hacerlo efectivo no pueden ser casuístas.

NUEVO CODIGO DE PROCEDIMIENTO PENAL

*Guillermo Alvarez Peñaloza**

Remontándonos a la reciente historia nacional, podemos manifestar a grandes rasgos, que dos fueron las principales justificaciones de la Reforma Constitucional de 1991:

La crisis del Congreso, ampliamente debatida por la opinión pública y por los medios de comunicación, y la crisis de la administración de justicia, aceptada, reconocida y estudiada por los entes del país.

El origen violento de nuestra sociedad desde los primeros tiempos del descubrimiento, parece ser el principio directo de la mencionada crisis. Un alto índice delincencial y uno de impunidad han sido las características uniformes de nuestra historia contemporánea. El diagnóstico aunque uniforme, ha tenido diferentes enfoques en relación con sus posibles soluciones. Como última tabla de salvación, parece ser el de enfocar el problema con una trascendental reforma constitucional. La Asamblea Nacional Constituyente decidió afrontar el reto y dio un vuelco en la administración de justicia creando

*Director de Seguridad Banco Cafetero.

la figura de la FISCALIA GENERAL DE LA NACION. Esta transformación conlleva la de actualizar las normas del Código de Procedimiento Penal vigente. La norma sustantiva no era necesario actualizarla. El Catálogo de delitos y sus penas, podría permanecer intacto. Por el contrario las normas de procedimiento, es decir, la forma y manera como se pone en ejercicio el Estatuto Penal, al variar el sistema de juzgamiento, era absolutamente indispensable actualizar al nuevo requerimiento.

El Artículo 5o. transitorio de la Nueva Constitución Nacional otorga al Presidente de la República facultades extraordinarias con el propósito de expedir todas las normas que organicen la Fiscalía General de la Nación y establecer igualmente nuevas disposiciones de orden procedimental.

El Ministro de Justicia encomienda la elaboración de un Anteproyecto de Ley a la Universidad de los Andes. Igualmente, nombra una Comisión Revisora con el propósito de puntualizar las críticas y opiniones sobre el trabajo inicial. En esta depuración intervinieron los diferentes Estamentos que tienen que ver con la administración de justicia. El 17 de agosto de 1991, se obtiene el primer texto del Proyecto que el Gobierno entrega a la Comisión. La Universidad de los Andes estudió el Anteproyecto durante cinco meses, mientras que la Comisión Revisora solo contó con una semana para adelantar este trabajo. La comisión especial nombró un Grupo de Ponentes y expidió un documento en el cual analiza cada Artículo del texto del Gobierno, enfatizando en los Artículos que no aceptaba.

La Comisión Especial se opuso a la incorporación en la jurisdicción ordinaria de temas muy polémicos, como: Jueces de Orden Público a la reserva de la identidad de los funcionarios judiciales, testigos e intervinientes en el proceso y a las limitaciones en el Derecho a la contradicción de la prueba. Esta discusión abarcó un término de tres meses.

Con base en el Trabajo de la Comisión Especial, el Ministerio de Justicia preparó un segundo proyecto que entregó a la misma comisión durante la

última semana de sus deliberaciones. En este nuevo Proyecto se tuvieron en cuenta muchas de las recomendaciones de la Comisión y en algunos aspectos se mejoró el Articulado inicial. Con este texto se iniciaron las discusiones Artículo por Artículo entre los componentes de la Comisión Especial y sus asesores y los representantes del Gobierno. Este estudio arrojó diferencias en los puntos comentados en los acápites anteriores, lo cual dio origen a un Acuerdo Político entre el Gobierno representado por el Ministro de Justicia y tres miembros de la Comisión Especial, en representación de las tres fuerzas políticas que intervinieron en la discusión. Para obtener un Acuerdo se celebró una reunión a puerta cerrada mientras que en otro recinto, al mismo tiempo, se seguía discutiendo cada una de las normas. Corría la última semana de sesiones de la Comisión Especial y no se sabía si habría o no Acuerdo para expedir el Código.

A la media noche del 27 de noviembre de 1991, el Ministro de Justicia comunicó que había logrado el Acuerdo sobre los puntos vitales de controversia. Al comenzar la revisión del Artículo 1o. "DEBIDO PROCESO" surgieron nuevas discrepancias que motivó la suspensión de las conversaciones. Al día siguiente, el Gobierno hizo entrega de un último texto, al que se le incorporaban las conversaciones discutidas y acordadas y que sería el texto que serviría de base para la votación. El Jueves 28 de noviembre, debía votarse el texto, ya que la Comisión tendría que aprobar el presupuesto y su período de sesiones terminaba el sábado 29 de noviembre. En ese momento ciertos sectores de la Comisión se oponían a votar el Código, pues pensaban que aún no existía Acuerdo en aspectos fundamentales. En una reunión cerrada se redactaron entre el Gobierno y tres miembros de la Comisión Especial, de afán, los Artículos que producían controversia. Con esos textos aprobados en esta reunión se pasó a la Plenaria para votación. Como era la hora de la comida, satisfaciendo esa necesidad se dio comienzo a la votación. Como ya existía un Acuerdo político la votación era solo un aspecto formal. En bloque inicialmente se aprobaron los Artículos que no ofrecía ningún problema. Posteriormente se estudiaron y se votaron los demás. Injustificadamente el

Artículo 344 se votó por partes dividiendo una misma frase. Negando inicialmente la expresión "Salvo caso de flagancia" y aprobando el resto. Como el resultado era absurdo, el texto original debió ser sometido a nueva votación, para terminar aprobándolo como aparece en la redacción definitiva.

A las cuatro de la madrugada concluyó el trabajo. Tan sólo restaba que el Presidente de la República procediera a darle expedición legal, lo que hizo por medio del Decreto No.2700 de 1991, el cual comenzó a regir el 1o. de julio de 1992.

CARACTERISTICAS DEL SISTEMA PROCESAL ANTERIOR

A grandes rasgos la estructura del sistema procesal anterior, ante la presencia de un reato criminoso cualquiera , era el siguiente:

- a) Intervenía la Policía Judicial, cuyas actuaciones eran la base o fundamento del proceso (Indagación Preliminar).
- b) El Juez de Instrucción asumía la responsabilidad de dirigir y orientar la investigación, legalmente era el único que podía practicar pruebas y resolver la situación jurídica del encartado (Sumario).
- c) Una vez perfeccionada la Investigación pasaba al Juez de conocimiento (Calificación -Audiencia Pública- Sentencia)

CAMBIOS DE LA NUEVA CONSTITUCION FRENTE A LA JUSTICIA

Los podemos sintetizar en tres fundamentales:

1. Creación de la Corte Constitucional.

2. Creación del Consejo Superior de la Judicatura.

3. Creación de la Fiscalía General de la Nación.

En cuanto a la Corte Constitucional. Se estableció en el Título VIII Capítulo 4o. Sus bases son las diferentes especialidades del Derecho. Los nombrará por períodos de ocho años el Senado de la República, de ternas que presenten el Presidente de la República, la Corte Suprema de Justicia y el Consejo de Estado. No podrán ser reelegidos. A la Corte Constitucional se le confía la guarda de la integridad y supremacía de la Constitución.

Se ha criticado con sobrada razón su origen eminentemente político, con el argumento fundamental de que es el principio de la politización del Poder Jurisdiccional. En efecto en la noche del 1o. de diciembre pasado, el Senado eligió la nueva Corte Constitucional compuesta por 6 magistrados liberales, dos magistrados conservadores y uno de la Alianza Democrática M-19.

Sobre el Consejo Superior de la Judicatura: Se divide en dos Salas: Una Administrativa integrada por seis Magistrados por un período de ocho años e integrada por dos Magistrados de la Corte Suprema de Justicia, un Magistrado por la Corte Constitucional y tres Magistrados por el Consejo de Estado.

Una Sala Jurisdiccional Disciplinaria integrada por siete Magistrados, nombrados para un período de ocho años por el Congreso Nacional de ternas enviadas por el Gobierno.

Las principales funciones del Consejo Superior son:

- Administrar la carrera judicial.
- Elaborar la lista de Candidatos para designación de funcionarios judiciales.

- Examinar la conducta y sancionar las faltas de los funcionarios de la rama judicial así como la de los abogados en ejercicio.
- Dirimir los conflictos de competencia entre las distintas jurisdicciones.

Fiscalía General de la Nación: Le corresponde investigar los delitos y acusar a los presuntos infractores ante los Juzgados y Tribunales competentes. Se exceptúan los delitos cometidos por Miembros de la Fuerza Pública en servicio activo o en relación con el servicio, el Presidente de la República, Ministros y Congresistas.

Está bajo la responsabilidad del Fiscal General: los Fiscales Delegados y los demás funcionarios que determine la Ley. El Fiscal General será elegido por 4 años por la Corte Suprema de Justicia, de terna enviada por el Presidente de la República y no podrá ser reelegido.

PRINCIPALES CAMBIOS EN EL NUEVO CODIGO

El cambio de sistema procesal en cuanto a la responsabilidad de la acusación, parece ser el principal cambio del nuevo Código.

El anterior Código con una tendencia inquisitiva, fundamentado en que la Jurisdicción es ejercida por jueces estables y permanentes en representación del Estado.

En el sistema acusatorio, la Jurisdicción será ejercida por Jueces o Jurados populares, a cuya cabeza aparece un nuevo ente acusador y especializado, la Fiscalía General de la Nación, independizando totalmente la función instructora de la función acusatoria y de juzgamiento.

El nuevo Código contiene algunos aspectos que no están todavía reglamentados, existe confusión en la interpretación de algunas normas y pocas contradictorias.

No se ha establecido plenamente el sistema acusatorio, lo que más se le aproxima es la División de funciones en el sentido de que la indagación previa, así como la investigación están a cargo de la Fiscalía y el Juzgamiento a cargo del Juez.

La Fiscalía General instruye y el Juez dicta la sentencia. No es acusatorio el sistema por las siguientes razones:

- a) La Fiscalía es autónoma.
- b) La Fiscalía administra justicia (Acusa o precluye el proceso).
- c) La Fiscalía hace lo mismo que hacían los jueces superiores (Resolución de detención -Libertad del Sindicato- Embargo de Bienes-).
- d) Investiga todos los delitos con excepción de lo establecido en el Artículo No.235 de la Constitución Nacional (La Corte Suprema de Justicia, juzga al Presidente, Congresistas, al Fiscal General). De acuerdo con el Artículo No.250 de la Constitución Nacional, tampoco juzga los delitos cometidos en ejercicio de sus funciones.

CAMBIOS DE ESTRUCTURA

1. La indagación preliminar no tiene término. No se abre investigación cuando no se ha podido identificar a los autores o partícipes. Mientras esto acontece, el proceso permanece en indagación preliminar.
2. Se mejoran indiscutiblemente las causales de prescripción y de inculabilidad.

3. No enumera pruebas judiciales, que se puedan practicar, dejándolas a las que expresamente cumpla la Ley.
4. Las entidades de control económico cumplen funciones de Policía Judicial, tal es el caso de la Superintendencia Bancaria, etc.
5. En la etapa de instrucción se permite la vinculación del tercero civilmente responsable.
6. No se deja establecido un término exacto de instrucción, por lo que se puede deducir que éste abarca hasta que prescriba la acción penal.
7. Al no tener un término exacto de cierre de investigación se presentan algunos problemas, como por ejemplo, con los bienes embargados por término indefinido.
8. Para cerrar la investigación tiene que haberse definido la situación jurídica de los sindicatos y una prueba mínima para calificar. No hay reapertura de la investigación, lo cual consideramos favorable.
9. La competencia de la Fiscalía se extiende hasta que quede ejecutoriada la Resolución acusatoria. La Fiscalía pierde su naturaleza y no hay justificación para mantener esta norma.
10. Al quedar ejecutoriada la Resolución de acusación, el Juez adquiere la competencia. Se presentan dos cambios:
 - El Fiscal que acusa entra como sujeto procesal y tiene que intervenir en la audiencia pública.
 - El primer acto procesal es un traslado de 30 días para pedir pruebas y nulidades. Consideramos buena esta disposición.

11. Qué sucedería cuando iniciada la etapa de juzgamiento y durante el término de pruebas, las aportadas en esta etapa son de tal magnitud que acaban con los argumentos jurídicos sobre los cuales se justificó el llamamiento a juicio o acusación?

Tres tesis se presentan para afrontar este problema jurídico:

- Decretar la nulidad.
- Absorver al sindicado.
- El Fiscal puede cambiar la Calificación sin que exista ningún recurso.

Consideramos más jurídica la tercera tesis, la cual es sustentada por el tratadista, doctor Jaime Bernal Cuellar.

12. La libertad del procesado es fundamental en el nuevo Código. Este aspecto está contemplado en los Artículos 28 al 32 de la nueva carta fundamental. El Artículo No.29 Tutela del nuevo proceso.
13. Garantiza el principio de la Reformatio - Impegus.
14. Ni siquiera excepcional se pueden prescindir de las garantías fundamentales, ni entregar el conocimiento a los militares.
15. Solamente la condena contra una persona determinada, se puede considerar como antecedente de tipo penal.
16. Prevalece el Derecho Sustancial sobre el Derecho Procesal. (Artículo No.228 Constitución Nacional).
17. La indemnización de perjuicios, presenta dificultad cuando existe pluralidad de sujetos.

18. La sentencia anticipada es una transacción entre el Fiscal y el Procesado. Solo puede haber transacción sobre circunstancias específicas y genéricas. No se puede bajar el mínimo de la pena.
19. La captura y las medidas de aseguramiento, son de resorte de la Fiscalía General.

Del estudio del nuevo estatuto he escogido algunos puntos importantes que considero, en forma muy general, deben ser conocidos por los funcionarios del sistema financiero a cuyo cargo, corresponden las áreas de seguridad.

Son unos comentarios ascendentes pero que no obedecen a ningún plan esquemático:

10. Se cambia el sistema general inquisitivo, por un sistema penal acusatorio. En el sistema inquisitivo la jurisdicción es ejercida por jueces permanentes y estables en representación del Estado. En el sistema acusatorio la jurisdicción será ejercida por jueces o jurados populares a cuya cabeza aparece un ente acusador especializado, la Fiscalía General, que trae como consecuencia la independencia total de la función acusatoria.
20. Con la vigencia del Código se separan definitivamente las funciones de acusación y juzgamiento, correspondiendo este último a un funcionario independiente de la etapa investigativa y que como Juez de Derecho determinará y definirá si hay o no lugar a la imposición de una pena o sanción.
30. El ejercicio de la acción penal se otorga a la Fiscalía General de la Nación. Con esta investidura le confiere las facultades de investigar, calificar y acusar en todas las "ACCIONES PENALES" que se presenten en el país.

-
40. La etapa de juzgamiento inicia cuando se haya proferido una RESOLUCION DE ACUSACION, debidamente ejecutoriada y a partir del 1o. de julio pasado, será función autónoma de un funcionario totalmente diferente: el Juez.
50. Se prevee la figura del desistimiento en dos eventos:
- En aquellos casos en que para iniciar la acción penal se deba instaurar una querrela por parte del sujeto pasivo o lesionado con el hecho punible.
 - En la reparación del daño o indemnización de perjuicios, especialmente en atentados de tipo económico.
60. Importante para el banco esta innovación del Código, ya que en los eventos en que se presente indemnización de índole económico, previa la reparación de los perjuicios materiales, se hace posible el desistimiento de la acción penal. Se establece pues, una importante excepción a la punibilidad de la acción penal.
70. En la vigencia del nuevo Código el Proceso Penal se inicia cuando el Fiscal Delegado profiera RESOLUCION DE APERTURA DE INVESTIGACION (Auto Cabeza de Proceso en el Código derogado). En este instante culmina la etapa de investigación previa, y se inicia realmente la investigación.
80. La nueva Constitución Nacional otorgó a la Fiscalía General, la facultad de asegurar la comparecencia de los presuntos sindicados, para hacer real tanto el restablecimiento del derecho como la indemnización de perjuicios, adoptando las medidas de aseguramiento y todas las demás que sean necesarias.

- 9o. El cumplimiento de las garantías constitucionales y los principios rectores del procedimiento penal, son las bases sobre las cuales el Fiscal adelantará la investigación correspondiente.
- 10o. Podrá el Fiscal cuando de la investigación se desprenda, o que el hecho no ha existido o que el sindicado no lo ha cometido, o que la conducta no es delito o que se presenta una causal excluyente de antijuridicidad o de culpabilidad, declarar la cesación del procedimiento, dando por terminada la investigación.
- 11o. En los procesos por delitos contra el Patrimonio Económico, cuya cuantía no sea superior a 100 salarios mínimos legales (excepto el hurto calificado y la extorsión), la acción penal se extinguirá para todos los sindicados cuando cualquiera repare el daño ocasionado.
- 12o. La etapa del juicio se inicia con la ejecutoria de la Resolución de Acusación y corresponde exclusivamente al Juez. El Fiscal debe sustentar la acusación ante el Juez.
- 13o. Los fiscales pueden, de acuerdo con la nueva Constitución, dictar las siguientes medidas de aseguramiento: Conminación, Caución y Detención Preventiva. Corresponde al Ministerio Público, vigilar el cumplimiento de estas normas evitando abusos de los fiscales, quienes ejercen la acción acusadora.

La acción civil para obtener el resarcimiento de los perjuicios morales o materiales consecuenciales al hecho criminoso, podrá ejercerse o ante la Jurisdicción Civil o dentro del proceso penal.

Tratándose del banco, cuando sea sujeto pasivo de una infracción de tipo penal, se deberá hacerse Parte Civil dentro del Proceso Penal, no sólo con el propósito de coadyuvar en el éxito de la investigación sino además en la obtención de la indemnización correspondiente.

Pertenece a la Dirección de Seguridad, de acuerdo con el Gerente de la Oficina lesionada, establecer los casos en que dentro de la acción penal se instaurara la Parte Civil en representación del Banco. Con el soporte de la Dirección General Jurídica se señalarán los honorarios en los casos en que la acción civil sea adelantada por abogados a tarifa.

140. La Constitución de Parte Civil podrá realizarse en cualquier momento, a partir de la resolución de apertura y hasta antes de que se profiera sentencia de segunda o única instancia.
150. El rechazo de la demanda de Parte Civil sólo podrá fundamentarse en la ilegitimidad de la Personería del demandante, cuando se establezca que se ha promovido independientemente la acción civil o cuando se acredite plenamente el pago de los perjuicios ocasionados con el hecho punible o la reparación del daño.
160. Los requisitos de la demanda de Parte Civil son los mismos exigidos por el Código de Procedimiento derogado, sin embargo debemos hacer énfasis en el numeral 7o. del Artículo 46 que exige una declaración juramentada de no haber incoado proceso ante la jurisdicción civil, tendiente a lograr la reparación de los daños y perjuicios consecuenciales a la violación del Estatuto Penal.

En efecto, cuando contra los intereses del banco, se presente un hecho del cual se pueden deducir tanto responsabilidad penal como la posibilidad de adelantar una acción de tipo civil, se debe estudiar previamente la conveniencia de optar por la acción que garantice en mejor forma el resarcimiento y recaudo de los dineros o bienes, teniendo siempre en cuenta que si se demanda civilmente, ya no sería jurídicamente posible, con posterioridad la constitución de Parte Civil dentro de la Acción penal por los mismos hechos y entre las mismas personas.

- 17o. La Parte Civil puede denunciar bienes en cualquier momento y el Fiscal decretará su embargo y secuestro, en la medida en que considere necesaria, previa prestación de la caución respectiva.
- 18o. En caso de que se hayan embargado bienes en exceso, en cualquier momento procesal podrá solicitarse el desembargo del exceso.
- 19o. Igualmente se decretará desembargo de bienes, cuando el encartado preste caución en dinero efectivo o mediante Póliza de Seguros por el monto que el funcionario judicial señale.
- 20o. Cuando se demuestre perjuicio dentro del proceso, el funcionario judicial debe liquidarlos, aún con el nombramiento de un perito si es necesario. Igualmente es susceptible de evaluarse los perjuicios morales. Si el sujeto pasivo ha promovido independientemente la acción civil, no se podrá imponer condena al pago de perjuicios.
- 21o. Cuando por Providencia ejecutoriada se haya declarado, o que el hecho causante del perjuicio no se realizó, que el sindicado no la cometió, que se obro en cumplimiento de un deber o en legítima defensa, la acción civil no podrá iniciarse ni proseguir.
- 22o. La Providencia que condene el pago de perjuicios, una vez ejecutoriada, prestará mérito ejecutivo ante los jueces civiles, cuando no hubiere bienes ni embargados ni secuestrados. Si existen bienes embargados o secuestrados, el Juez Penal remitirá la actuación al Juez Civil para que proceda al remate de tales bienes.
- 23o. El Sindicado no podrá enajenar bienes sujetos a registro durante el año siguiente contados a partir de su vinculación jurídica, a menos que justifique y garantice la indemnización de perjuicios o se hubiese demostrado su inocencia.

-
- 24o. Acreditada la propiedad, la posesión o tenencia legítima del objeto material o instrumento del delito, el funcionario judicial ordenará de plano la devolución de los mismos. Este aspecto es importante, ya que en aquellos casos en que se obtengan recuperaciones de dinero o elementos de propiedad del banco, demostrando sumariamente la legitimidad de la tenencia por parte de la Institución, el funcionario judicial sin más consideraciones, deberá devolver esos elementos al Banco.
 - 25o. Igualmente el funcionario judicial, en cualquier momento del proceso, cuando se demuestre que los Títulos de propiedad sobre bienes sujetos a registro, fueron obtenidos fraudulentamente, ordenará la cancelación de los títulos y del registro respectivo. Igual cancelación se realizará sobre los Títulos-Valores sujetos a registros obtenidos indebidamente.
 - 26o. La acción civil que se deriva del hecho punible, se extinguirá en todo o parte por cualquiera de los modos consagrados en el Código Civil.
 - 27o. Sindicado es aquella persona natural a quien se le atribuya participación en el hecho punible. Adquiere esta calidad desde su vinculación de indagatoria o de declaratoria de persona ausente.
 - 28o. Defensor, salvo las excepciones legales, debe ser un abogado inscrito.
 - 29o. Bajo su responsabilidad tanto el defensor como el apoderado de la Parte Civil podrán designar suplentes. El nombramiento del suplente se entiende revocado cuando se designe a otra persona. Los apoderados principales y suplentes no pueden actuar al mismo tiempo.
 - 30o. En la instrucción del proceso se pueden utilizar medios mecánicos, electrónicos y técnicos, teniendo en cuenta que no atenten contra la dignidad humana y garantías constitucionales. Las diligencias pueden ser recogidas y conservadas en audio-video y si es necesario su contenido se llevará por escrito. Los despachos judiciales podrán utilizar

las técnicas de administración e informática judicial. En las diligencias se podrá utilizar mecanismos técnicos tendientes a garantizar la protección y reserva de la identidad de las personas que intervienen.

Los memoriales dirigidos por los abogados no requieren presentación personal.

- 31o. La actuación se realizará por escrito y en idioma castellano. Si estuviere en otro idioma o la persona no se exprese en castellano, se hará la traducción o se utilizará un intérprete. Se iniciará con el nombre de la Entidad que practica la diligencia, lugar, hora, día, mes y año en que se realice y las de quienes intervinieron. Si no sabe firmar, se le tomará la huella digital. En caso de negativa a firmar lo hará un testigo. Si la diligencia fuese realizada por un medio técnico, se levantará un acta en que conste la fecha y la hora y se le suscribirá por las partes.
- 32o. Todas las diligencias se realizarán por duplicado. El recurso de apelación se surtirá por original. Cuando se aporten documentos originales o únicos, se llevará copia o fotocopia autenticada por el Secretario.
- 33o. Por causa justificada la práctica de una diligencia se puede suspender. De este hecho se dejará constancia y se citará día y hora en que se deba reiniciar.
- 34o. Toda actuación o diligencia que se practique con el sindicado, sin la presencia de su defensor, se considerará inexistente. Se exceptúa la versión libre y espontánea en caso de captura en flagrancia.
- 35o. Toda persona está obligada a comparecer ante el funcionario judicial. Su desobediencia será sancionada con arresto de uno a treinta días.

-
- 36o. Las citaciones se realizarán en los medios y forma que el funcionario considere eficaces, indicando fecha, hora y las sanciones en caso de desobediencia.
 - 37o. Las copias de las providencias presumen tanto la existencia de la actuación, como de las pruebas en las cuales se fundamentan.
 - 38o. Los términos procesales se contarán de acuerdo con el calendario. Todos los días y horas son hábiles para practicar diligencias.
 - 39o. Las providencias de los funcionarios judiciales son: Resoluciones, Autos y Sentencias. Si deciden sobre el objeto del proceso serán sentencias. Si resuelven algún aspecto sustancial o incidente serán Autos Interlocutorios. Los de simple trámite serán de sustanciación y las proferidas por el Fiscal serán Resoluciones.
 - 40o. Las notificaciones son: Personales, por estado, por edicto, por conducta concluyente y en estrados.
 - 41o. Los recursos en el nuevo procedimiento son: Reposición, apelación y de hecho, que se instaurarán por escrito.
 - 42o. Para que no se declare desierto el recurso de apelación en la segunda instancia, necesariamente debe sustentarse.
 - 43o. Las sentencias absolutorias dictadas por cualquier Juez deben ser consultadas con el superior cuando no haya intervenido Parte Civil dentro del proceso.
 - 44o. El proceso tiene dos instancias, la primera generalmente ante Juez singular o ad-quo y la segunda instancia generalmente ante Juez plural o ad-qued.

- 45o. Toda determinación judicial debe estar fundamentada en pruebas, recepcionadas en forma regular y oportunamente allegadas al informativo.
- 46o. Para poder condenar a un sindicado se necesita haber recaudado dentro del proceso una prueba que lleve a la certeza del hecho denunciado y a la responsabilidad del sindicado.
- 47o. En la etapa de instrucción habrá reserva del sumario, la cual se levantará durante la etapa de juzgamiento.
- 48o. La prueba aportada legalmente dentro de una actuación, podrá trasladarse a otra actuación en copia autenticada.
- 49o. La inspección tiene por objeto comprobar el estado de las personas, los lugares, rastros u otros efectos materiales de utilidad para el esclarecimiento de los hechos. Igualmente establecer los partícipes del mismo. Se extenderá un Acta que consigne todo lo actuado.
- 50o. La prueba pericial se adelantará por personas que tengan experiencia técnica o artística, es decir, con conocimientos especiales y que sirvan para aclarar circunstancias propias de la investigación.
- 51o. Los peritos emitirán un dictamen claro, preciso y detallado. No podrán en ningún evento emitir ningún tipo de juicio sobre la responsabilidad penal.
- 52o. Los documentos mediante los cuales se establezcan circunstancias procesales, se agregarán en original o copia auténtica. También dentro de la inspección en caso de no ser posible en otro momento, tomando preferencialmente el original y dejando copia.

-
- 53o. Las personas que tengan en su poder documentos, tienen la obligación de entregarlos, o de permitir su conocimiento al funcionario que lo solicite. Si se trata de personas jurídicas, la orden de entrega de documentos se notificará al representante legal.
- 54o. Toda persona natural está obligada a rendir testimonio dentro del proceso penal, salvo las excepciones constitucionales y legales. Cuando se trate de personas jurídicas, el testimonio será rendido por el representante legal o su apoderado. Igualmente deben rendir testimonio todas las personas que hayan tenido conocimiento de lo investigado. No están obligados a declarar contra sí mismo o contra su esposa o compañera permanente o parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil. Tampoco están obligados a declarar los Ministros de cualquier culto, los abogados y las personas que deban guardar secretos.
- 55o. El funcionario judicial no podrá sugerir respuestas, ni formular preguntas capciosas, ni ejercer violencia sobre el testigo.
- 56o. Para que la confesión sea válida se requiere:
- a) Realizarla ante funcionario judicial.
 - b) Que la persona sindicada esté asistida de su defensor.
 - c) Que la persona haya sido enterada del derecho que tiene a no declarar contra sí mismo.
 - d) Que se haga en forma consciente y libre.
- 57o. Quien confiese la ejecución de un hecho delictuoso, se le reducirá la condena hasta una tercera parte.

- 58o. El indicio es aquel hecho del cual se infiere la presencia de otro hecho, se basa en la experiencia y supone un hecho indicador. El hecho indicador es indivisible.
- 59o. La Policía Judicial está constituida por: La Policía Judicial de la Policía Nacional, el Cuerpo Técnico de Investigación de la Fiscalía General de la Nación y todos los servidores públicos que integran las unidades fiscales y el DAS.
- 60o. Ejercen funciones especiales de Policía Judicial, la Contraloría y la Procuraduría General de la Nación. Las autoridades de tránsito en asuntos de su competencia. Las entidades públicas que ejercen funciones de vigilancia y control. Los alcaldes e Inspectores de Policía.
- 61o. En los casos de flagrancia y en el lugar de los hechos, la Policía Judicial podrá ordenar y practicar pruebas sin necesidad de providencia previa. Iniciada la instrucción sólo actuará por orden del Fiscal.
- 62o. Durante la investigación previa habrá reserva sumarial, salvo para el defensor del imputado que rinda versión preliminar.
- 63o. Durante la etapa de investigación previa se podrán practicar todas las diligencias tendientes a establecer el esclarecimiento de los hechos denunciados.
- 64o. No existe término para la duración de la investigación previa. Esta etapa se extenderá hasta que exista prueba para dictar resolución inhibitoria o mérito para vincular como parte dentro de la investigación al imputado.
- 65o. La Resolución de apertura o la inhibitoria solo podrán ser dictadas por el Fiscal o Unidad de Fiscalía.

-
- 66o. Con autorización del Fiscal, el Jefe de la Unidad de Fiscalía podrá suspender la investigación previa si transcurridos 180 días no existe mérito para dictar Resolución de Apertura.
- 67o. El Fiscal se abstendrá de iniciar la instrucción cuando aparezca:
- a) Que el hecho no ha existido.
 - b) Que la conducta es atípica.
 - c) Que la acción penal no puede iniciarse.
 - d) Que está plenamente demostrada una causal excluyente de antijuridicidad o culpabilidad.

Esta decisión se tomará por auto interlocutorio que tiene recurso de apelación. Esta figura constituye indiscutiblemente, otro tipo de prescripción extraordinaria.

- 68o. Corresponde al funcionario que haya intervenido en la investigación previa, en caso de ser competente, asumir la investigación y adelantar la instrucción, mientras no prescriba la acción.
- 69o. Durante la instrucción existirá reserva de la actuación, salvo solicitud en contra de autoridad competente para actualizar procesos judiciales, administrativos o disciplinarios o tramitar el recurso de hecho.
- 70o. Quien viole la reserva sumarial incurrirá en multa de 1 a 5 salarios mínimos. La publicación en algún medio de comunicación de información reservada, constituirá presunción de la violación de la reserva.

- 71o. El funcionario competente tiene la obligación de investigar tanto lo favorable como lo desfavorable para los intereses del sindicado y las partes que intervienen.
- 72o. Los instrumentos y efectos con los que se cometió algún hecho punible y que no tengan libre comercio, pasarán a poder de la Fiscalía General de la Nación o a la Fiscalía que esta designe.
- 73o. Cuando se investigue el tipo penal de falsedad en títulos de propiedad de un bien sometido a registro o un tipo penal de estafa, el funcionario judicial podrá decretar el embargo, independiente de la medida de aseguramiento.
- 74o. Tanto los allanamientos como el registro, la retención de correspondencia o la interceptación de comunicaciones telefónicas, no se darán a conocer a las partes cuando el funcionario lo considere prudente.
- 75o. Cuando sea procedente un allanamiento, el funcionario judicial lo ordenará por medio de providencia motivada, sin que sea necesario ninguna notificación.
- 76o. En caso de flagrancia en el momento de cometer un delito en lugar no abierto al público, la policía judicial podrá ingresar sin orden escrita del Fiscal. De todas las diligencias de allanamiento se levantará un acta.
- 77o. La interceptación de comunicaciones (telefónicas, radiotelefónicas y similares) debe ser aprobada por la Dirección Nacional de Fiscalías. Las grabaciones se trasladarán al expediente por medio de escrito. En caso de flagrancia las autoridades de Policía Judicial podrán interceptar y reproducir las comunicaciones.
- 78o. El funcionario judicial recibirá indagatoria a las personas que por antecedentes y hechos que aparezcan en el informativo o por flagrancia,

considere como autores o partícipes. La persona que tenga en su contra alguna imputación puede solicitar su propia indagatoria.

- 79o. La indagatoria se surtirá siempre con abogado, salvo que el imputado se encuentre en peligro de muerte.
- 80o. El reconocimiento fotográfico se hará con un número no inferior a seis fotografías y si de su realización resultare algún reconocimiento, las fotografías se agregarán a la actuación.
- 81o. Se puede capturar en flagrancia cuando el individuo es sorprendido al momento de cometer el hecho o con objetos, instrumentos o huellas de los cuales se pueda deducir que momentos antes ha cometido un delito o participado en él. Puede ser capturado por cualquier persona. Por ningún motivo el capturado puede permanecer por más de 36 horas por cuenta de una persona diferente al Fiscal o al Juez.
- 82o. Los derechos del capturado son y sobre ellos se debe dejar constancia escrita:
- a) Motivo de la captura.
 - b) Derecho a entrevistarse inmediatamente con un defensor.
 - c) Derecho de comunicarse con la persona a quien él considere se le debe informar su detención.
 - d) Si se trata de investigación previa, tiene derecho de rendir una versión libre, pudiendo guardar silencio sobre los motivos de la incriminación. Esta versión sólo se puede hacer ante el defensor.
 - e) Derecho a no ser incomunicado.

- 83o. El Fiscal que haya impartido orden de captura debe cancelarla inmediatamente cuando cesen los motivos que dieron lugar a ella.
- 84o. No podrá resolverse la situación jurídica sin que previamente se haya oído en descargos o indagatoria al imputado, o se le haya declarado como persona ausente.
- 85o. El término para oír en indagatoria es a más tardar dentro de los tres días siguientes en que el capturado haya sido puesto a órdenes del Fiscal. Si por los mismos hechos hay más de dos capturados, se duplica este término.
- 86o. Dentro de los 5 días siguientes deberá resolverse la situación jurídica al capturado. Si el encartado no está detenido este término se puede ampliar hasta 10 días.
- 87o. Habrá lugar a detención preventiva en los siguientes casos:
- Para todos los delitos de competencia de Jueces Regionales (antes denominados sin rostro).
 - Cuando el delito tenga prevista pena de prisión con una duración mínima de dos años.
 - En algunos delitos especiales, entre otros: falsificación de moneda nacional o extranjera, tráfico de moneda falsificada, pánico económico, hurto agravado.
- 88o. Quien injustamente haya sido privado de la libertad, podrá demandar al Estado por indemnización de perjuicios.
- 89o. Están exentos de libertad provisional entre otros delitos los siguientes: Peculado por Apropiación, Fraude Procesal, Falsificación de moneda

nacional o extranjera, tráficos de moneda extranjera, pánico económico, hurto calificado.

- 90o. El Habeas Corpus es una acción pública que tutela o resguarda la libertad personal del capturado, con violación de las garantías constitucionales o legales; o la prolongación indebida de su detención.
- 91o. Jamás podrá cerrarse o darse por terminada una investigación, sin que previamente se haya resuelto la situación jurídica del sindicado.
- 92o. El sumario se calificará o dictando resolución de acusación o resolución de preclusión de la instrucción.
- 93o. Ejecutada la resolución de acusación, la competencia la adquieren los jueces que deban juzgar. El Fiscal pierde la dirección de la investigación, adquiriendo la calidad de sujeto procesal.
- 94o. Toda persona se presume inocente hasta tanto judicialmente no se le haya declarado responsable. La duda se resuelve a favor del imputado.
- 95o. La ejecución de la pena consecuencial a la sentencia ejecutoriada, corresponde a la Dirección General de Prisiones.

Para el autor de esta ponencia es materia de mucho orgullo profesional, el haber podido presentar ante todos ustedes este trabajo jurídico, el cual sintetiza no sólo mi experiencia profesional de 21 años continuos como responsable del área de Seguridad del Banco Cafetero, sino además, durante este mismo tiempo mi experiencia judicial.

No ha sido fácil realizar 11 Seminarios Nacionales y han sido muchos los obstáculos y dificultades que se han tenido que superar.

No obstante lo anterior, desde este mismo momento con optimismo y camaradería, esperamos el Doceavo Seminario Nacional de Seguridad del Sector Financiero bajo la dirección de la Asociación Bancaria y de Entidades Financieras de Colombia, evento que como este, indefectiblemente será un éxito.

PLANES DE APOYO E INTERACCION DE LA POLICIA CON EL SECTOR FINANCIERO

*Carlos Alberto Otálora Avendaño**

SISTEMAS DE ALARMAS

Objetivos:

- Diseñar e implementar en forma gradual una modalidad funcional y eficiente a nivel técnico, operativo y administrativo para el servicio de atención de alarmas prestado por la Institución a las personas naturales y jurídicas que lo soliciten.
- Unificar y estandarizar el manejo técnico, operativo y administrativo del servicio de control de alarmas en todo el país.
- Impartir instrucciones y fijar responsabilidades para el diseño, implementación y puesta en marcha del nuevo sistema.

*Coordinador de Acercamiento Policía Nacional

- Adecuar gradualmente los sistemas de atención de alarmas existentes a nivel nacional, para sustituirlos por el señalado en la presente directiva.

SISTEMAS UTILIZADOS

a) Ciudades con C.A.D. Cali , Barranquilla y Santafé de Bogotá

Funciona al obturar un botón localizado en el lugar donde se produce el incidente, acción que genera una señal eléctrica, que viaja por línea telefónica (par aislado) hasta el lugar donde se tiene el equipo que la recibe y la convierte en señal luminosa y/o audible. El operador de la policía acciona el archivo de alarmas del C.A.D., el sistema reconoce la dirección y envía automáticamente el caso al despachador que tiene a su cargo el control de las patrullas en ese sector de la ciudad y éste a su vez, por radio informa a la patrulla más cercana para que atienda el caso.

En Medellín, el usuario es el responsable del mantenimiento e instalación de los elementos del interior del banco, líneas de transmisión, equipo receptor y convertidor de la señal eléctrica. En esta ciudad con el sistema se tienen cuatro (4) ventajas bien definidas como son:

- Registro automático de la hora de obturación de la alarma e impresión de la misma.
- Economía de un agente 24 horas al día.
- Ingreso de un sólo contratista para el mantenimiento del equipo de traductor.
- Apoyo económico de la Asociación Bancaria de Medellín, por intermedio de un Fondo de Seguridad manejado por esa entidad para tal fin.

Los usuarios del sistema en Medellín, pagan a la Policía Nacional \$7.166.30, mensuales que ingresan a Fondos Internos de la Dirección Administrativa. Adicionalmente las entidades aportan una cuota al Fondo de Seguridad Bancaria para apoyo al mantenimiento y renovación de equipos del Departamento.

Santafé de Bogotá: El sistema de alarma en Bogotá se encuentra originado por tres formas:

Primer Sistema: El de pares aislados, ubicado en la Sexta Estación, es el mismo descrito al comienzo.

Segundo Sistema: El sistema del PBX, en la actualidad viene funcionando bajo el mismo principio del par aislado, agregando un elemento técnico ubicado en la Empresa de Teléfonos de Bogotá, identificado como (PBX Distribuidor Automático de Llamadas), el cual envía la señal, llegando automáticamente a un microcomputador ubicado en el C.A.D.

Este microcomputador fue donado a la Policía Nacional por la firma "ALARMSEG INGENIERIA LTDA". quienes poseen todo el paquete de instrucciones, programas y diseños, son los únicos que hacen el registro de las alarmas que mediante elaboración de contrato realiza la Policía Nacional para Bogotá.

Objetivos del Sistema a Utilizar: Según la Directiva Permanente No. 032 del 111192, requiere establecer un sistema a través del cual la alarma se conecta a un microcomputador por medio de un PBX, que tenga un determinado número de líneas telefónicas y responden a números iguales.

Se acciona con la obturación de un botón o al levantar el auricular del teléfono de la **Entidad o Persona** en situación de emergencia afiliada al sistema policial.

La marcación se genera automáticamente con acceso directo al microcomputador localizado en el C.A.D. o en la Estación 100, información que se transfiere al sistema de esta unidad a través del formato previo correspondiente con la información requerida para atender el caso.

Se sugiere a lo anterior para asumir el control directo del microcomputador tomar en su totalidad el lenguaje de máquina (HANDWARE) y así mismo los paquetes, programas, instrucción y diseños (SOFTWARE), hacer los ajustes, estudios y cambios correspondientes para la ampliación del sistema a través de ingenieros de sistemas y el mantenimiento como lo establece la directiva; los ingresos provenientes de este servicio pueden canalizarse en el mantenimiento de los equipos y al desarrollo propio de la tecnología policial.

Tercer Sistema: Es el de grabación al número 112 de la Policía Nacional, C.A.D., la cual es asegurada por un elemento mecánico electromecánico o electrónico, dirigido por una línea telefónica particular o que automáticamente hace la marcación, previo programa del número 112, este sistema a los Centros Automáticos del Despacho trae desventajas y consecuencias graves, debido a la gran afluencia de tráfico, no es confiable y también produce procedimientos de falsas alarmas no comprobables.

Se sugiere a lo anterior la destinación y adquisición de uno o más abonados (líneas telefónicas), para que se destine a este servicio de atención de alarmas.

b) Ciudades Capitales sin C.A.D.

En estas ciudades el sistema de alarmas es muy similar al que opera en Cali y Barranquilla, las diferencias básicas están dadas por la pérdida de todos los archivos con información relativa al banco, tampoco permite registros automáticos de tiempos relacionados con la atención del incidente. La inexistencia de registros automáticos hace que los críticos de la emergencia, (hora en que se dispara la alarma y hora en que se hace presente la policía), se tengan que registrar manualmente en un libro.

El despacho de las patrullas, se efectúa desde la respectiva estación CIEN (E-100) o sala de radio.

Los elementos que conforman el sistema en estas ciudades, se diferencia de los que le corresponde a la Policía, donde el C.A.D., en reemplazo por un equipo de radio, es decir que los sensores en los bancos, las líneas telefónicas y las cajas receptoras de señales luminosas y/o audibles, siguen siendo las mismas de los otros sistemas. Esta diferencia hace la tarifa en estas ciudades sea menor.

c) Alarmas en otras Poblaciones

Los elementos siguen siendo los mismos del sistema anterior, la diferencia, radica principalmente en el despacho de la patrulla, la cual sale normalmente del mismo cuartel.

El caso se atiende con el personal disponible. Estas patrullas generalmente no tienen radio y las líneas telefónicas, la mayoría de las veces son cables físicos.

Actualmente a nivel nacional, se benefician del servicio de control de alarmas 64 entidades vinculadas a través de contrato, así:

- Instalada a la Central de Radio de la respectivas unidades.
- Instalada al Centro Automático del Despacho.

Igualmente, mediante la línea del 112 se atienden las llamadas de emergencia sin mediación de contrato ni cobro de tarifa alguna.

ASALTO A ENTIDADES FINANCIERAS

Causa: Al analizar las causas concretas para la comisión de este ilícito es necesario abordar el tema desde dos perspectivas; las víctimas y los victimarios.

a) Víctimas

Las entidades financieras afectadas han comprobado, en muchos casos, la famosa teoría criminológica de la "oportunidad" por las siguientes razones:

- Se toman muy a la ligera las recomendaciones impartidas por los organismos de seguridad respecto a la rigurosidad en los estudios de seguridad del personal que va a desempeñar las labores de vigilancia y el personal que labora en el banco o corporaciones, al igual que realizar (se pasa por alto) esporádicamente y al azar nuevos estudios de seguridad.
- Las investigaciones sobre casos de hurto a entidades financieras han comprobado la hipótesis que señala como coautores o cómplices del delito a personal interno o vigilantes.
- No se evalúan los mecanismos de seguridad humanos y técnicos, para adecuarlos a las necesidades de la zona y los modus operandi de los delincuentes.
- Inadecuada coordinación entre las empresas de vigilancia de entidades financieras y organismos de seguridad del Estado, que dificultan las investigaciones e impiden tomar medidas de carácter preventivo.

b) Victimarios

Las causas próximas para que sucedan hechos como el que se analiza, son claramente identificados así:

- **Cambios ideológicos en el mundo.** Los acontecimientos, sucedidos en Rusia necesariamente afectaron a los movimientos revolucionarios de América Latina, en el sentido de haber disminuido el apoyo económico y logístico por parte de estos países; situación que los llevó a buscar otras estrategias, entre las que se encuentran los asaltos a entidades financieras.
- **Población "cesante" del narcotráfico.** Los golpes dados al narcotráfico, con la muerte de varios de sus principales cabecillas y captura de otros, dejaron sin actividad a un gran número de delincuentes altamente entrenados y con armas sofisticadas, dedicados al sicariato, paramilitarismos y secuestro selectivo, esa población dirigió su accionar hacia el secuestro y asalto bancario por ser las modalidades que mayores ganancias les representa y con relativo riesgo.
- **Población "desmovilizada" de la guerrilla.** La falta de planeación para la organización de los programas de reincursión de guerrilleros amnistiados, dejó gran número de individuos sin ninguna perspectiva social y sólo con la alternativa de convertirse en delincuentes comunes aprovechando la experiencia adquirida en su actividad como guerrillero.

Además es bien conocido, que en muchos casos el guerrillero no se acostumbra a las ganancias de un negocio subsidiado por el Estado y desea continuar con los mismos ingresos de su vida anterior.

c) **Motivos**

Ligados a los anteriores planteamientos se encuentran los "motivos" para la comisión de este ilícito:

- El mantener el nivel de ingreso que proporciona el narcotráfico y la actividad guerrillera.
- El delincuente conoce mejor que cualquier ejecutivo de una empresa las fortalezas y debilidades en cuanto a seguridad, dentro de las que se encuentran la capacidad de infiltrarse, o extorsionar y ello es aprovechado (oportunidad) y sirve de motivación para que se cometa el ilícito.

ANALISIS ESTADISTICO

Ayuda 1

Total 1991:	379
Promedio mensual:	31
Total 1992:	285 (010192 - 251192)
Promedio mensual:	26
Variación país:	-16%

Nota: Se tomaron promedios mensuales para comparar períodos de tiempo iguales.

Ayuda 2

De acuerdo a la entidad afectada es bien significativo que en los dos años el porcentaje más elevado correspondió a entidades crediticias. Para 1992 el porcentaje fue del 63% representado en 180 casos, en comparación con bancos que sumaron 105 hurtos.

Ayuda 3

La disminución en el número de casos, como consecuencias en el decremento de la cuantía hurtada.

Para 1992, la mayor cuantía se hurtó en la Metropolitana del Valle de Aburrá, \$789'296.825 a bancos \$1.122'464.276 a corporaciones igual comportamiento registro esta zona en 1991.

Comparando los dos años, se tiene que las regiones con mayores cuantías en un número de casos reducido fueron Norte de Santander y Santander que registran cuantías de \$908.488.000 en 8 casos y \$369'516.500 en 15 respectivamente.

Ayuda 4

Tomando como punto de referencia las jurisdicciones que corresponden a cada Departamento de Policía y registrando promedios mensuales para cada año, se observa que las áreas de mayor frecuencia en asaltos bancarios son las mismas para los dos años, aunque en cada una se presentaron variaciones.

Las ciudades son: Metropolitana del Valle de Aburrá, Metropolitana de Bogotá, Metropolitana de Cali, departamento de Antioquia, departamento de Santander y departamento de Atlántico.

Exceptuando a la metropolitana de Cali, las restantes zonas presentan disminución, aunque continúan llevando el protagonismo en el número de ilícitos.

Ayuda 5

Continuando en el análisis geográfico se tiene que los municipios más afectados en 1992 fueron, en orden descendente:

- Medellín: Con 90 casos que representan el 31.6% del total ocurrido en este período de tiempo.
- Bogotá: Registró 75 ilícitos, equivalentes al 26.3%.
- Cali: Con 32 hurtos y un porcentaje de participación del 11.2%.
- Barranquilla: Se cometieron 12 hechos equivalentes al 4.2%.
- Bucaramanga: Con 12 hechos que representan el 4.2%.

Como se observa el 77.4% de los hurtos a entidades financieras se cometieron en las 5 principales ciudades del país, situación que ubica este delito como de tendencia urbana, pero con la combinación de la delincuencia común y guerrillera.

Ayuda 6

Para un análisis más riguroso sobre los asaltos a entidades financieras, es necesario señalar cuál entidad exactamente fue la más afectada para así tomar medidas de control y prevención de manera particular.

La Caja Agraria ha sido el objetivo en el mayor número de casos, 27 en 1992 y le siguen el Banco Cafetero, Colpatria y Conavi.

Es de anotar que todas estas entidades, al conocer estadísticas tan dramáticas, están en mora de tomar medidas drásticas, empezando por depuración de personal, para detectar infiltrados o posibles sobornables y aún a quienes pueden estar extorsionando especialmente en el sector rural.

Ayuda 7

El mayor incremento en orden cronológico se presentó entre junio y julio del 106%. Para el último período, octubre y noviembre la variación fue del 25%.

**FRECUENCIA DE ENTIDADES AFECTADAS POR
DEPARTAMENTO**

DEPARTAMENTO	Frecuencia	Porcentaje
ANTIOQUIA	11	3.9
ARAUCA	3	1.1
ATLANTICO	12	4.2
CALDAS	2	.7
CAQUETA	1	.4
CAUCA	1	.4
CESAR	5	1.8
CHOCO	1	.4
CUNDINAMARCA	4	1.4
GUAJIRA	1	.4
NARIÑO	2	.7
NORTE DE SANTANDER	8	2.8
QUINDIO	1	.4
RISARALDA	6	2.1
SANTANDER	15	5.3
TOLIMA	6	2.1
HUILA	1	.4
URABA	2	.7
VALLE	1	.4
VICHADA	1	.4
SANTAFE DE BOGOTA D.C.	75	26.3
CALI	32	11.2
VALLE DE ABURRA	94	33.0
TOTAL	285	100.0

FRECUENCIA DE HURTO A ENTIDADES POR MUNICIPIO

MUNICIPIO	Frecuencia	Porcentaje
ABREGO	1	.4
AMAGA	1	.4
APARTADO	2	.7
ARMENIA	1	.4
BARRANCA	3	1.1
BARRANQUILLA	12	4.2
BELEN UMBRIA	1	.4
BETULIA	1	.4
BOGOTA	75	26.3
BOSCONIA	1	.4
BUCARAMANGA	12	4.2
BUGA	1	.4
CALI	32	11.2
CHIRIGUA	1	.4
CUCUTA	3	1.1
DOSQUEBRADAS	1	.4
EL CARMEN	2	.7
EL CHARCO	1	.4
EL COPEY	1	.4
EL RETIRO	1	.4
ENVIGADO	2	.7
FLORENCIA	1	.4
FORTUL	1	.4
GIRARDOT	2	.7
GRANADA	1	.4
GUAMO	1	.4
HACARI	1	.4
HELICONIA	1	.4

FRECUENCIA DE HURTO A ENTIDADES POR MUNICIPIO

MUNICIPIO	Frecuencia	Porcentaje
HOBO	1	.4
IBAGUE	4	1.4
ITAGUI	2	.7
IZCUANDE	1	.4
JURADO	1	.4
LIBORINA	1	.4
MANIZALES	2	.7
MEDELLIN	90	31.6
MEDINA	1	.4
MELGAR	1	.4
OCAÑA	2	.7
PEREIRA	4	1.4
PTO RONDON	1	.4
RIONEGRO	1	.4
SAN ALBERTO	1	.4
SAN PEDRO	1	.4
SARAVENA	1	.4
STA. BARBARA	1	.4
STA. ROSA	1	.4
TIMBIO	1	.4
VALLEDUPAR	1	.4
YALI	1	.4
ZAPATOCA	1	.4
TOTAL	285	100.0

FRECUENCIA DE ENTIDADES AFECTADAS

ENTIDAD	Frecuencia	Porcentaje
AGRARIA	27	9.5
AHORRAMAS	8	2.8
ANGLOCOLOMBIANO	5	1.8
BANCOQUIA	15	5.3
BCH	5	1.8
BIC	7	2.5
BOGOTA	10	3.5
CAFETERO	20	7.0
CALDAS	3	1.1
CITIBANK	2	.7
COCENTRAL	1	.4
COLMENA	5	1.8
COLOMBIA	7	2.5
COLPATRIA	18	6.3
COMERCIO	2	.7
CONAVI	17	6.0
CONCASA	7	2.5
COOPDESARROLLO	9	3.2
COOPERATIVO	2	.7
COOPSIBATE	5	1.8
CORPAVI	15	5.3
CREDISOCIAL	2	.7
DAVIVIENDA	10	3.5
ESTADO	2	.7
FINANCIACOP	2	.7
GANADERO	8	2.8
GRANAHORRAR	13	4.6
OCCIDENTE	4	1.4

POPULAR	11	3.9
SOCIAL AHORROS	14	4.9
SUDAMERIS	4	1.4
TEQUENDAMA	1	.4
TRABAJADORES	2	.7
UCONAL	6	2.1
VILLAS	16	5.6
TOTAL	285	100.0

**TENDENCIA DE ASALTO A ENTIDADES BANCARIAS
DURANTE 1992**

MES	Frecuencia	Porcentaje
ENERO	30	10.5
FEBRERO	32	11.2
MARZO	28	9.8
ABRIL	16	5.6
MAYO	23	8.1
JUNIO	15	5.3
JULIO	31	10.9
AGOSTO	28	9.8
SEPTIEMBRE	21	7.4
OCTUBRE	27	9.5
NOVIEMBRE	34	11.9
TOTAL	285	100.00

TOTAL VALOR HURTADO \$3.238'242.349

TOTAL VALOR RECUPERADO \$58'850.800

FRECUENCIA DE ENTIDADES HURTADAS

ENTIDAD	Frecuencia	Porcentaje
BANCOS	105	36.8
CORPORACIONES	180	63.2
TOTAL	285	100.0

PREVENCION DE FRAUDE CON TARJETAS DE PAGO Y CHEQUES DE VIAJERO

*Paul Bolívar**

CARACTERISTICAS DE LA TARJETA**

American Express emite tres clases de Tarjetas: la Tarjeta Personal (verde), la Tarjeta Oro y la Tarjeta Platino. Las Tarjetas Personales están emitidas en 28 monedas. Estas son Tarjetas de pago, y no de crédito. Las facturas son pagaderas en su totalidad al recibo del extracto mensual.

Sus características son:

- **Intransferible:** Sólo tiene derecho a utilizarla la persona cuyo nombre figura impreso en relieve en el anverso de la Tarjeta.
- **Número de Identificación de la Tarjeta:** Este número sirve para el control inventario de los plásticos. El número impreso de cuenta del Titular y este número de identificación de la Tarjeta pueden ser

* Jefe Investigaciones América Latina y el Caribe, American Express.

** Casos de American Express

asociados interiormente para verificar la validez de la Tarjeta (medida de seguridad).

- **Tintas Ultravioletas:** Si se examina una Tarjeta genuina de American Express bajo luz ultravioleta, aparecerán en fluorescencia tanto las letras AMEX como la figura del centurión.
- **Figura del Centurión:** Proporciona gran seguridad, puesto que presenta un alto grado de claridad y detalle.
- **Número de Cuenta del Titular:** Tiene 15 dígitos, empezando por "37", que identifica a la Compañía American Express. El prefijo "34" también ha sido reservado para el uso de American Express y comenzó a emitirse a finales de 1988.
- **Fechas de Validez:** La Tarjeta no puede ser utilizada ni antes ni después de la fecha de validez.
- **Titular Desde:** Refleja el año en que se le emitió al Titular la Tarjeta por primera vez.
- **Propiedad de American Express:** Esta nota indica el derecho de American Express a retirar la Tarjeta en cualquier momento.
- **Banda Magnética:** Contiene información codificada electrónicamente sobre la cuenta.
- **Panel de Firma:** Cualquier borradura, intento de falsificación o manipulación efectuada sobre este panel produce la aparición de la palabra "VOID" que significa "NULO", quedando con ello anulada la Tarjeta.
- **Número de Cuenta Duplicado:** Se encuentra grabado en el reverso de la Tarjeta; tiene que ser idéntico al que figura en el anverso, asegurando que éste no ha sido alterado.

TARJETA OPTIMA SM

En el mes de marzo de 1987, American Express anunció su plan de lanzar al mercado un nuevo tipo de Tarjeta llamada la Tarjeta Optima, emitida como compañera de las existentes actualmente, Tarjeta Platino, Tarjeta Oro y Tarjeta Personal (verde). Sus características son:

- a) Los favorables tipos de interés para el usuario en los pagos aplazados, vinculados al tipo preferencial (ajustado semestralmente);
- b) Línea de crédito individualizada;
- c) Facturación detallada;
- d) Privilegios para anticipos en metálico.

La Tarjeta Optima es una Tarjeta de Crédito, vulnerable a todos los sistemas de fraude que atacan a otros tipos de Tarjetas. Además, no se puede ser Titular de la Tarjeta Optima, como un Titular básico o suplementario al menos que sea ya Titular de Tarjeta American Express con buena reputación, por lo menos durante un año (obsérvese la fecha de aniversario). Hay tres Tarjetas Optimas diseñadas como compañera de la Tarjeta Personal (verde), Tarjeta Oro y Tarjeta Platino.

USO FRAUDULENTO DE TARJETAS

Pérdidas y/o Sustracción: Normalmente la pérdida o sustracción de una Tarjeta están asociadas con pérdidas directas de otras propiedades y documentación de sus titulares. La mayoría de las veces la pérdida viene originada por otro delito. Y así la recuperación de una Tarjeta puede ser una importante pista en la solución de un delito más importante. Una llamada telefónica a una de nuestras Oficinas de Inspección y Seguridad puede resolver el caso. Algunas Tarjetas son substraídas del correo. Estas Tarjetas

tienen un alto riesgo potencial de fraude, puesto que ni el Titular ni el emisor de la Tarjeta tienen conocimiento de la pérdida o sustracción.

Tarjetas Alteradas: El plástico es físicamente alterado imprimiendo en relieve sobre la Tarjeta nuevos datos (otros nombres y números). Existen varias fuentes para obtener esta información, incluyendo el papel carbón obtenido de notas de cargo o crédito. Si el número de la Tarjeta impreso en relieve aparece alterado, el número de cuenta duplicado, grabado en bajo relieve en el reverso de la Tarjeta American Express, puede servir para su comparación y detección.

Afeitado y Pegado: Cualquier número de caracteres alfa-numéricos es cortado con una cuchilla de afeitar de la superficie de la tarjeta, pegándolos con tipos de pegamento que secan rápidamente. Se efectúa este procedimiento, normalmente, para colocar en la tarjeta un número de cuenta válido, completamente diferente y/o cambiar el nombre, pudiendo ser utilizada como identificación o para el cobro de cheques. Una llamada a la Oficina local de Inspección y Seguridad de American Express puede resolver el tema. En este caso y en otros como este, es esencial comprobar que el número de cuenta coincide con el nombre del Titular. Si resulta sospechoso, examine la cara frontal de la Tarjeta en busca de las señales de los números y letras originales, exceso de pegamento, etc. Examine el reverso de la Tarjeta para comprobar si coincide el número de cuenta. En el caso de que esté borrado, examine la superficie de la Tarjeta en sentido oblicuo a la luz, puesto que los caracteres impresos originalmente todavía aparecerán en el reverso del plástico. Como en todos los casos de sospecha de Tarjetas alteradas, preste particular atención a la colocación de cualquier tipo de etiquetas, como los "stickers" de compañías aéreas, etc., usadas para enmascarar la alteración. Sepa, así mismo que con un poco de habilidad se puede producir una Tarjeta perfectamente pasable. Las herramientas utilizadas para este método de alteración suelen ser de tipo artístico como un escalpelo, navajas de afeitar y un cristal de aumento iluminado.

TARJETA OPTIMA SM

En el mes de marzo de 1987, American Express anunció su plan de lanzar al mercado un nuevo tipo de Tarjeta llamada la Tarjeta Optima, emitida como compañera de las existentes actualmente, Tarjeta Platino, Tarjeta Oro y Tarjeta Personal (verde). Sus características son:

- a) Los favorables tipos de interés para el usuario en los pagos aplazados, vinculados al tipo preferencial (ajustado semestralmente);
- b) Línea de crédito individualizada;
- c) Facturación detallada;
- d) Privilegios para anticipos en metálico.

La Tarjeta Optima es una Tarjeta de Crédito, vulnerable a todos los sistemas de fraude que atacan a otros tipos de Tarjetas. Además, no se puede ser Titular de la Tarjeta Optima, como un Titular básico o suplementario al menos que sea ya Titular de Tarjeta American Express con buena reputación, por lo menos durante un año (obsérvese la fecha de aniversario). Hay tres Tarjetas Optimas diseñadas como compañera de la Tarjeta Personal (verde), Tarjeta Oro y Tarjeta Platino.

USO FRAUDULENTO DE TARJETAS

Pérdidas y/o Sustracción: Normalmente la pérdida o sustracción de una Tarjeta están asociadas con pérdidas directas de otras propiedades y documentación de sus titulares. La mayoría de las veces la pérdida viene originada por otro delito. Y así la recuperación de una Tarjeta puede ser una importante pista en la solución de un delito más importante. Una llamada telefónica a una de nuestras Oficinas de Inspección y Seguridad puede resolver el caso. Algunas Tarjetas son substraídas del correo. Estas Tarjetas

tienen un alto riesgo potencial de fraude, puesto que ni el Titular ni el emisor de la Tarjeta tienen conocimiento de la pérdida o sustracción.

Tarjetas Alteradas: El plástico es físicamente alterado imprimiendo en relieve sobre la Tarjeta nuevos datos (otros nombres y números). Existen varias fuentes para obtener esta información, incluyendo el papel carbón obtenido de notas de cargo o crédito. Si el número de la Tarjeta impreso en relieve aparece alterado, el número de cuenta duplicado, grabado en bajo relieve en el reverso de la Tarjeta American Express, puede servir para su comparación y detección.

Afeitado y Pegado: Cualquier número de caracteres alfa-numéricos es cortado con una cuchilla de afeitar de la superficie de la tarjeta, pegándolos con tipos de pegamento que secan rápidamente. Se efectúa este procedimiento, normalmente, para colocar en la tarjeta un número de cuenta válido, completamente diferente y/o cambiar el nombre, pudiendo ser utilizada como identificación o para el cobro de cheques. Una llamada a la Oficina local de Inspección y Seguridad de American Express puede resolver el tema. En este caso y en otros como este, es esencial comprobar que el número de cuenta coincide con el nombre del Titular. Si resulta sospechoso, examine la cara frontal de la Tarjeta en busca de las señales de los números y letras originales, exceso de pegamento, etc. Examine el reverso de la Tarjeta para comprobar si coincide el número de cuenta. En el caso de que esté borrado, examine la superficie de la Tarjeta en sentido oblicuo a la luz, puesto que los caracteres impresos originalmente todavía aparecerán en el reverso del plástico. Como en todos los casos de sospecha de Tarjetas alteradas, preste particular atención a la colocación de cualquier tipo de etiquetas, como los "stickers" de compañías aéreas, etc., usadas para enmascarar la alteración. Sepa, así mismo que con un poco de habilidad se puede producir una Tarjeta perfectamente pasable. Las herramientas utilizadas para este método de alteración suelen ser de tipo artístico como un escalpelo, navajas de afeitar y un cristal de aumento iluminado.

Planchado y/o Reimpresión en relieve: El objeto de este procedimiento, que empezó a proliferar a principio de 1980, consiste en alisar el plástico para eliminar los caracteres alfa numéricos impresos en relieve. Las Tarjetas de plástico, compuestas básicamente de polivinilocloruro, se hacen más elásticas cuando están expuestas al calor. Por lo tanto, se utilizan varias fuentes de calor (desde una plancha de uso doméstico, una vela, un soldador, agua caliente, hasta un microondas); después se ejerce presión sobre el plástico (con una prensa mecánica o hidráulica). Antes de aplicar el calor y la presión, el falsificador debe quitar el existente relieve de color de los caracteres, normalmente negro o color oro: una variedad de abrasivos son usados para este propósito, los más comunes son los productos de limpieza del hogar, los cuales poseen un material, piedra pómez, disuelto en una base de detergente. Si el relieve no es borrado, las señales de los viejos caracteres serían visibles. Otra herramienta necesaria para este procedimiento es una mesa de impresión en relieve. Existen varios modelos con distintos estilos mecanográficos, con las que trafican varias redes de delincuentes. Algunas de estas máquinas de imprimir tienen la capacidad de "planchar" caracteres existentes, comparable a una cinta correctora de máquina eléctrica de escribir.

TARJETAS FALSAS

Aunque no se considere técnicamente una falsificación, los plásticos en blanco del tamaño de las Tarjetas han sido usados fraudulentamente con la colaboración de comerciantes corruptos que los aceptan. Estos casos toman el nombre de fraudes de "Plástico Blanco".

La única herramienta necesaria es una máquina de imprimir. Sólo puede tener éxito cuando existe la complicidad con algún comerciante. Cualquiera que posea un plástico, del tamaño de una Tarjeta de Crédito con información impresa en relieve, como número de cuenta, nombre, etc., está probablemente envuelto en algún fraude y debería ser investigado.

Llamamos Tarjetas falsas o falsificadas a aquellas cuyo plástico e impresión es totalmente falso. Históricamente surgieron de organizaciones delictivas que tenían acceso a grandes posibilidades litográficas. Anteriormente utilizaron pantallas de seda como medios de producción. Sin embargo, la complejidad actual del diseño de las Tarjetas ha minimizado el tipo de falsificación con pantallas de seda.

Si sospecha que una Tarjeta es falsificada, examine la Tarjeta con todos los rasgos expuestos anteriormente. Una llamada telefónica a la Oficina local de Inspección y Seguridad de American Express puede resolver rápidamente la cuestión.

EXAMEN DEL CAMPO

Un individuo en posesión de varias Tarjetas de Crédito e identificaciones a nombre de diferentes personas puede ser un usuario de Tarjetas substraídas. Aunque también puede tratarse de un especialista, profesional de solicitudes falsas (ver definición más adelante).

Examine la Tarjeta. Una impresión confusa y con escasez de definición puede ser un indicio de Tarjeta falsificada. Particularmente, observe las áreas de la Tarjeta que tiene finas líneas de impresión en busca de borrones o colores desiguales. Una prueba adicional consistiría en mirar la Tarjeta bajo una luz ultravioleta.

Observe los caracteres impresos en relieve. ¿Están muy espaciados o fuera de la línea? Busque "señales" de números que fueron borrados. Si esto no se manifiesta fácilmente en el reverso de la Tarjeta, mire el anverso de la misma. Es útil ladear ligeramente la Tarjeta para que la luz la ilumine oblicuamente. Si tales señales son detectadas, esto es un fuerte indicio de que la Tarjeta ha sido alterada. Busque también cualquier deformación del plástico. Esta distorsión puede ser causada por el exceso de calor durante el proceso de alteración.

Examine siempre el panel de firma en busca de alguna señal de falsificación. La mayoría de estas son pulverizadas con pintura o se les aplica algún corrector líquido blanco. En otras ocasiones es adherido un nuevo panel de firma utilizando una cinta adhesiva. Busque simples intentos de borraduras o signos de utilización de productos químicos.

Si se detecta cualquiera de estos indicios estaría justificada una investigación más profunda.

LOS RASTROS DEL PLASTICO

El uso de una Tarjeta por un individuo deja un claro rastro. A menudo este uso, el cual coloca a un individuo en un lugar y día específico, puede ser una pista que sirva de prueba para el procesamiento por otros delitos.

Para obtener datos sobre la Tarjeta de American Express, en los casos en que American Express misma no está entre las víctimas, en la mayoría de los países es necesaria una orden judicial. Sería conveniente solicitar orientación a través de la Oficina más cercana de Inspección y Seguridad de American Express.

FRAUDE CON TRAVELERS CHEQUES

El Cheque de Viajero "Travelers Cheque" es un instrumento financiero o medio de pago creado por American Express en 1981. Proporciona al público una alternativa conveniente y segura de transportar dinero. Ya que, a diferencia del dinero en efectivo, el valor de los Travelers Cheques perdidos o sustraídos es reembolsado. Técnicamente un Travelers Cheque de American Express es una orden de retirar dinero del emisor para pagar al tenedor o portador la suma indicada en el Cheque. Únicamente es negociable cuando es contra-firmado por el comprador de origen, y puede ser pagable a la orden de cualquiera designado por el comprador, a la hora de utilizarlo, mediante endoso.

Los Travelers Cheques de American Express son actualmente vendidos en las siguientes monedas:

1. Dólares Americanos
2. Dólares Canadienses
3. Francos Franceses
4. Francos Suizos
5. Libras Esterlinas
6. Marcos Alemanes
7. Yens Japoneses
8. Riyales Saudíes
9. ECU (Unidad Monetaria Europea).

Existen varios importes en todas las monedas.

Todos los Travelers Cheques de emisión actual de American Express están impresos sobre un papel especial con marca al agua. El texto, el borde y dibujo en la cara del Cheque están impresos con un grabado de acero, el cual proporciona un efecto de realce y un énfasis nítido y claro de los detalles. El Travelers Cheque de American Express lleva en la parte inferior caracteres de microcódigos impresos en tinta magnética para permitir su manejo automático.

Los Travelers Cheques de American Express no tienen fecha de caducidad. Por lo tanto, incluso las emisiones antiguas pueden continuar siendo presentados al cobro indefinidamente.

A continuación señalamos algunas de las protecciones de los Travelers Cheques de American Express.

Firma y/o Contrafirma: Busque borraduras, alteraciones, faltas de ortografía, trazos o correcciones.

Las planchas de imprimir son grabadas: La figura del Gladiador destaca nítidamente y contiene aproximadamente 2.000 trazos grabados. Pase sus dedos por encima de las palabras "American Express Travelers Cheque" y note la textura de las letras en relieve. El color de la tinta utilizada es de alta calidad en color y textura.

Los importes y divisas: están impresos en el anverso y reverso.

Marca al agua: "AMEXCO".

Test de frotar: Moje un dedo y frote el recuadro del importe en la parte posterior del Cheque.

USO FRAUDULENTO DE LOS CHEQUES

1. Los Cheques perdidos y substraídos están generalmente asociados a pérdidas de otras propiedades de los clientes. Cuando son substraídos están normalmente relacionados con otros delitos.
2. Las pérdidas en blanco tienen origen en sustracciones y robos de productos a la venta y remesas desaparecidas en tránsito. Otro tipo es el "hurto" que se suele producir en un banco o institución financiera mediante la distracción de los empleados. La clave del éxito de los delincuentes en los hurtos y grandes butrones consiste en la habilidad de viajar. Las víctimas son seleccionadas en pequeñas áreas urbanas donde tal actividad era anteriormente rara o desconocida.

El Departamento de Inspección y Seguridad de American Express puede desempeñar un papel de vital importancia para el éxito policial en estas situaciones, actuando como centro de dispersión de información a las distintas Brigadas, Comisarías y Puestos de la Guardia Civil.

3. Con solicitudes fraudulentas de reembolso también se intentan estafas. Un comprador de Travelers Cheque denuncia sus Cheques como perdidos o sustraídos y solicita un reembolso habiendo cobrado ya él mismo los Cheques, o por medio de un cómplice, o cobrándolos posteriormente.
4. Falsificación: A causa de la liquidez del Cheque, American Express es con frecuencia víctima de falsificación cometida por falsificadores de papel moneda. En aquellos casos donde un Cheque es sospechoso, deberían ser aplicados previamente los tests de campos (tes de frotar, etc.). Una llamada al Departamento de Inspección y Seguridad de American Express le resolverá cualquier duda.
5. Características del Cobro Fraudulento.
 - a) Las borraduras o eliminación química de la firma que se encuentra en el ángulo superior izquierdo;
 - b) El uso de un rotulador disimula las alteraciones o sobretraza la firma;
 - c) La técnica de la "pluma seca" utilizada por negociadores experimentados a la hora de efectuar el cobro. La contrafirma ya ha sido trazada o simulada: el negociador con una pluma o bolígrafo seco pretende simular que firma.

Como en las Tarjetas, los Travelers Cheques cobrados, documentos asociados con ellos y otros datos son a menudo de un extraordinario valor en las investigaciones de otras actividades delictivas.

Para obtener tal información en la mayoría de los países es necesaria una orden judicial, pero solamente en los casos en que American Express no es también víctima. Las solicitudes de información deben dirigirse a la Oficina de Inspección y Seguridad de American Express más próxima.

TERMINOLOGIA USADA COMUNMENTE

Acquiring Bank/Banco Adquisitivo: Afilia comercios, los cuales aceptan tarjetas bancarias. Algunos Bancos Adquisitivos pueden también ser Bancos Emisores.

Additional Cardmember/Titular Suplementario: Son miembros Suplementarios autorizados por el Titular Básico a efectuar cargos contra la cuenta Básica y realizados con sus propias Tarjetas.

Anniversary Date/Fecha Aniversario: Es el año en que fue emitida la Tarjeta por primera vez. Se encuentra impreso después del encabezamiento "Member since"/"Titular desde".

Aproval Code/Código de Aprobación: Para una transacción de American Express, el número de la esquina superior derecha que aparece en el formulario de la nota de Cargo ("ROC"), indica que una transacción fue autorizada por el Sistema de Autorización de Crédito (CAS). La transacción CAS es recuperable desde los logaritmos del ordenador mostrando la fecha, la hora, dirección del comercio, la cantidad y la acción tomada.

Authorization/Autorización: Para las transacciones de American Express, existen Oficinas centrales designadas para recibir, normalmente por teléfono, y revisar peticiones de establecimientos (comercios) para autorizaciones de

crédito. Muchas transacciones son actualmente manejadas directamente por un ordenador con un campo de aprobación programado. Aquellas autorizaciones que se encuentren fuera de este campo son referidas a los autorizadores, los cuales autorizan o no la transacción.

Automated Teller Machine/Cajero Automático: Un dispositivo activado por una banda magnética impulsa un cargo en tarjeta de crédito o de pago. Conectada a una base de datos central puede realizar varias operaciones bancarias, incluyendo disposición de dinero en efectivo y a veces entre instituciones financieras.

Los Cajeros de American Express pueden también proporcionar Travelers Cheques emitidos por ésta.

Bankcard/Tarjeta Bancaria: Es una tarjeta de crédito emitida por los bancos miembros o instituciones financieras, por ejemplo, Visa y Mastercard.

Basic Cardmember/Titular Básico: Es el titular que se hace responsable de los cargos efectuados por el Titular y cualquier otro Titular Suplementario de la cuenta.

Bust-Out Merchant/Comercio "Quebrado": Un comercio que se afilia a un emisor de Tarjetas y que no efectúa negocio legal alguno, sino que coopera con otros delincuentes en el fraude.

Cancellation/Cancelación: Finalización voluntaria o involuntaria de una relación entre el Titular de una Tarjeta o Establecimiento (comercio) y American Express.

Chargeback/Devolución de Cargo: Es un ajuste para deducir importes de la cuenta de un Establecimiento (comercio), cuando el Emisor devuelve una factura por no haber autorizado la transacción.

Charge Card/Tarjeta de Pago: Tipo de Tarjeta emitida por American Express, Diners Club y Carte Blanche. Las facturas son debitadas al recibirlas.

Collusive Merchant/Comercio Confabulado: Establecimiento que conspira con terceros para estafar a un emisor de Tarjetas. A menudo no se intercambian mercancías, sino que las ganancias del fraude son compartidas en metálico.

Counterfeit Card/Tarjeta Falsificada: Una Tarjeta totalmente falsa creada con técnicas conocidas de falsificación, tales como pantallas de seda o foto-offset (litografía).

Billing/Facturación: Un sistema por el cual, en la mayoría de las veces, el Titular de American Express recibe la copia "dura" del cargo que firmó, con su listado de facturación.

Descriptive Billing/Facturación Descriptiva: La información sobre transacciones individuales es descrita en el estado de facturación del Titular.

Discount Rate/Tanto por Ciento de Descuento: Es el porcentaje de cada venta que el establecimiento (comercio) paga al emisor de Tarjetas o Banco Adquisitivo.

Embossing/Impresión en relieve: El proceso de imprimir caracteres sobre un plástico.

Floor Limit/Límite: El importe de una venta convenida en contrato entre el emisor y el comercio a partir de la cual este está obligado a pedir autorización. Normalmente el emisor no aceptará el cargo si no ha sido cumplido este requisito.

Fraudulent Application /Solicitud Fraudulenta: Una solicitud de Tarjeta complementada con información falsa con el propósito de engañar y hacer fraude.

Hologram/Holograma: Una imagen producida con láser que tiene la apariencia tridimensional y alternativa. Es utilizado como mecanismo de seguridad en algunas tarjetas bancarias.

Imprinter/Impresora: Una máquina usada por un Establecimiento (comercio) para imprimir una Tarjeta de Crédito o Pago sobre un cargo con la fecha de la transacción, número de Establecimiento, nombre y dirección.

Issuer/Emisor: Compañía que emite Tarjetas o Travelers Cheques.

Issuing Bank/Banco Emisor: Miembro bancario o institución financiera que afilia individuos a Tarjeta de Crédito. Algunos Bancos Emisores pueden ser a la vez Bancos Adquisitivos, es decir, que afilian comercios.

Lithography/Litografía: Reproducir por el método foto-offset, utilizando una imagen negativa (foto) quemada en una plancha sensible a la luz. Con esta técnica se consigue un producto de alta calidad.

Magnetic Stripe/Banda Magnética: Aparece en las Tarjetas de American Express en la parte superior del reverso de la misma. Contiene información codificada, la cual sólo puede ser interpretada por un lector compatible. Varía información es codificada, incluyendo el nombre del Titular, fecha de validez, etc.

Non-Received Card/Tarjeta No-Recibida: Una Tarjeta sustraída en su camino hacia el Titular, normalmente en el correo. Su pérdida es inicialmente desconocida tanto por el titular como por el emisor.

Personal Identification Number (PIN)/Número Personal de Identificación (PIN): A veces llamado Código Personal de Identificación (PIC), un código alfa y/o numérico utilizado para identificar al presentador de la Tarjeta usando una terminal. La mayoría de los números PIN son utilizados en Cajeros Automáticos o en el caso de American Express, en máquinas expendedoras de Travelers Cheques.

Purchase Agreement Form (PAF)/Factura de Compra: Complementada por el comprador de Travelers Cheques, contiene las cantidades, números de series de Cheques vendidos, lugar de venta y nombre del comprador.

Record Of Charge (ROC)/Nota de Cargo: Formulario compuesto de dos o tres partes que son firmados por el Titular como pago en el punto de venta. También es llamado talón de cargo factura o ticket de venta.

Sing & Travel Account/Cuenta-Firme y Viaje: Opción de pago ofrecida por American Express a Titulares de la Tarjeta Personal, Tarjeta Oro y Tarjeta Platino permitiendo que el mismo pague un viaje aéreo o de otro tipo en cómodos plazos.

Silk Screening/Pantalla de Seda: Proceso legítimo de impresión utilizado en falsificación. El trabajo artístico es colocado en una pantalla porosa y los colores son introducidos a través de la misma. Históricamente producía Tarjetas bancarias pasables. Recientes cambios en los diseños de Tarjetas bancarias han derrotado este tipo de falsificación.

Slug/Regleta: La placa de metal impresa en relieve en la máquina que imprime los cargos detalla el nombre del comercio, localización y número de Establecimiento asignado por los emisores, cuyas Tarjetas son aceptadas por dichos Establecimientos.

Summary Of Charges (SOC)/Remesa de Cargos: Formulario presentado por un Establecimiento afiliado a American Express, que contiene en un resumen el importe de las notas de cargo que adjuntan.

Unique Embossed Character/Unico Carácter Impreso: Es ahora utilizado por algunos emisores como medida disuasoria a la falsificación. Consiste en imprimir un carácter, el cual es propiedad exclusiva del emisor y no se encuentra fácilmente disponible en el mercado.

Warning Bulletin/Boletín de Alerta: Es un boletín de Tarjetas canceladas, perdidas o substraídas, distribuidos a comercios por un emisor de Tarjetas. También es llamado Boletín de Cancelación.

White Plastic/Plástico Blanco: Un plástico del tamaño de una Tarjeta de crédito o de pago (polivinilocloruro) sobre la cual se puede imprimir y después es utilizado por comercios confabulados con otros estafadores o actuando aisladamente.

APENDICE: ¡Pida Ayuda!

Hoy en día los profesionales de la investigación y protectores de la Ley tienen que ser más polifacéticos que sus predecesores. La clave del éxito radica en tener la habilidad de localizar la ayuda experta tan pronto como sea posible.

A las Oficinas de Inspección y Seguridad de Europa, con sus respectivas Areas de responsabilidad, por favor, tómese la libertad de contactarlas directamente. Si es necesario llame a cobro revertido. Le podrán ayudar a obtener las respuestas a sus preguntas y la asistencia que necesite.

Desde 1984 al Servicio Secreto de los Estados Unidos se le ha encomendado como principal misión dentro de la protección de las Leyes Federales, aquellas relacionadas con los delitos cometidos con Tarjetas de crédito o pago en los

Estados Unidos. También pueden intervenir y ayudar en investigaciones adicionales si fuere necesario.

El F.B.I. es responsable en Estados Unidos de la protección de ciertas Leyes Federales relacionadas con delitos con Travellers Cheques.

En Europa varios componentes de los Servicios de Investigación Criminal están encargados de la protección de las Leyes relacionadas con delitos cometidos con Tarjetas de crédito o de pago, fraude con Travellers Cheques, falsificación, etc. Las Comunicaciones directamente o a través de Interpol (ICPO - OPIC) son muy efectivas, así como lo es la relación con las oficinas de Inspección y Seguridad de American Express.

ESTRUCTURA DE LA CAPACITACION Y EL SISTEMA DE DESARROLLO DE PERSONAL EN LAS EMPRESAS

*Nelson Alvear Altamirano**

Un panorama del Sistema de Desarrollo de Personal que se realiza en la empresa podrá diseñarse al responder las siguientes preguntas:

- Los empleados manifiestan que la capacitación es una herramienta útil para su propio progreso dentro de la empresa antes que un período de descanso o de alejamiento de la rutina del trabajo?
- Con la capacitación se busca satisfacer una estructura de metas de los empleados y de la empresa antes que montar programas porque "hay que hacer algo"?
- La empresa ha modificado sustancialmente sus ofrecimientos de Capacitación en los últimos 4 años?
- Cuando se han efectuado cambios, la nueva capacitación ha consultado las necesidades de los empleados?

* Capacitador Desarrollo de Personal. Banco de Bogotá.

- Se ha elaborado un inventario de los empleados para medir necesidades de capacitación?
- Tanto la organización como los empleados tienen metas claras sobre el tipo de capacitación que debe suministrarse?
- Los empleados tienen planes concretos para su futuro desarrollo profesional para los cuales se puede recomendar capacitación?
- Los empleados saben a quién recurrir para consejería sobre programas de adiestramiento?
- Los jefes y supervisores conocen los programas y políticas de capacitación?
- Se elaboran estudios de seguimiento para evaluar los resultados de la capacitación?
- Se registra quién recibe adiestramiento y de qué clase para determinar cómo debe ser utilizado por la empresa?
- Los sistemas de compensación, transferencia, promoción etc. van ligados a un sistema de capacitación?

Si la mayoría de estas preguntas se responden con NO, el sistema de capacitación se está usando como un medio inócuo (placebo), para males que no están suficientemente definidos.

Por lo tanto, es necesario administrar la capacitación como estrategia para el desarrollo de personas dentro de la empresa, que beneficie tanto al empleado como a la organización y que permita realizar importantes decisiones sobre el mejor uso del tiempo de capacitación así como de su presupuesto y recursos humanos.

1. Políticas Tradicionales de Capacitación

Existen 3 tipos tradicionales de capacitación que pueden ofrecer programas apropiados en ciertas circunstancias pero no conducen al logro del máximo desarrollo del Recurso Humano y pueden generar altos costos.

- Capacitación en habilidades específicas del trabajo

Busca mejorar las habilidades en el trabajo corriente, generalmente a través de aprendizaje en clase. Este enfoque puede ser esencial para la organización y tiene la ventaja de presentar resultados fácilmente medibles en términos de incremento de habilidades para las tareas.

Sin embargo, cuando los empleados ya han aprendido a realizar las labores de su puesto, se preguntan: " Que más hay". Si la empresa no piensa en el paso siguiente puede estar perdiendo la inversión colocada en esa capacitación y se corre el riesgo que los empleados entrenados abandonen la empresa por falta de nuevos campos de acción en su trabajo.

- Capacitación como un beneficio general

Se piensa que la capacitación es un beneficio marginal que se otorga al empleado sin importar el valor que pueda tener su aprendizaje. En este enfoque se ofrece a los empleados una variedad de posibilidades que van desde programas de capacitación en el hogar hasta cursos impartidos en instituciones externas. Los empleados pueden solicitar su propio programa de capacitación dentro de límites de tiempo y presupuesto. En este enfoque puede existir un costo menor de inversión y el tiempo libre del empleado y de la empresa es aprovechado. Sin embargo, si estos programas no se enmarcan dentro de las necesidades de desarrollo de carrera individual y organizacional se corre el riesgo que los empleados "prueben de todo" y esto no les sirva en su ocupación.

- Capacitación como estímulo

Consiste en otorgar incentivos por desempeño o con fines de promoción generalmente en los niveles altos de la compañía mediante conferencias, pagos de matrículas, seminarios de aprendizaje avanzado, u otros beneficios educativos.

El problema radica en que estas decisiones sobre Capacitación, muchas veces se basan en factores que no se relacionan con las necesidades individuales u organizacionales o con los beneficios mutuos para empleado y empresa.

Este tipo de Capacitación demuestra altruismo empresarial pero no enfoca muy bien el desarrollo de los recursos de la organización.

2. Una aproximación más segura

La capacitación es más efectiva cuando se imparte dentro de un Programa de Desarrollo de Carrera Ocupacional cuidadosamente planeado.

La consecuencia inmediata consiste en que se presenta una oportunidad para que el empleado seleccione aquellos programas de capacitación que satisfagan sus necesidades inmediatas y contribuya hacia futuras metas. Por parte de la empresa, surge mayor posibilidad de evaluar las capacidades individuales del personal y utilizarlas en las tareas de la organización.

Si la capacitación es parte del desarrollo de una carrera se convierte en un fin en sí misma. La forma de proceder en este caso sería la siguiente:

- Necesitamos actualización en X aspecto
- Quién desea y necesita utilizar esta información ahora y en el futuro ?
- Se busca un programa que sirva para esta situación

- Terminado el programa se asignan proyectos especiales a los asistentes

De esta manera el adiestramiento dentro de un Sistema de Desarrollo de Carrera permite que la organización decida quién quiere ser entrenado, quién debe ser entrenado, en qué áreas, cómo y cuándo es el uso de su entrenamiento.

En el Desarrollo de Carrera, la capacitación mira a largo plazo, por lo tanto, el aprendizaje formal en cursos o seminarios es sólo una herramienta que debe ser complementada con el aprendizaje que ocurre a través de procesos informales.

Muchas compañías están utilizando recursos que de hecho pierden por no registrar los datos de reemplazos, entrenamientos después de ascensos o rotación de puestos, lo cual constituye verdadera Capacitación e inversión.

Así pues, cuando la capacitación persigue un desarrollo de carrera presenta dos beneficios fundamentales.

- Permite que el empleado decida sobre el tipo de capacitación que elije.
- Permite que la empresa suministre un repertorio más amplio de estrategias de capacitación.

LA ELECCION POR PARTE DEL EMPLEADO

Los empleados deben hacer preguntas que les suministren elementos para decidir sobre su capacitación, tales como:

- Cuáles son mis opciones para adquirir este conocimiento o habilidad dentro y fuera de la empresa?
- Debo excluir algunas opciones por restricciones de tiempo, costos, políticas organizativas?

- Conozco suficientemente las opciones de Capacitación que me presenta la empresa para poder escoger? Si no, dónde las puedo encontrar y a quién debo recurrir?
- Con respecto a mis metas, cómo organizo estas opciones con relación a tiempo y progreso potencial?
- Algunas de esas opciones son mejores que otras para utilizar el aprendizaje que voy a adquirir?
- Para aprovechar mis conocimientos y experiencias pasadas qué tipo de entrenamiento es mejor? el formal, la experiencia o la guía de otros.

LA OFERTA DE PROGRAMAS POR PARTE DE LA EMPRESA

La empresa puede ofrecer programas de capacitación bajo 3 modalidades.

1. Modalidad de Capacitación basada en Cursos

Consiste en el diseño de programas para impartir conocimientos y habilidades en áreas específicas de trabajo que hagan competentes a los empleados para desempeñar puestos. Esta modalidad se puede impartir mediante 2 programas.

- Capacitación interna o cursos especiales de la empresa.
- Capacitación externa o Cursos impartidos fuera de la empresa.

2. Modalidad de Capacitación basada en la Experiencia

Esta categoría capacita al personal mediante el "aprendizaje por la acción" en el puesto, rotación de puestos, o mediante la asignación de proyectos especiales.

Esta modalidad se puede impartir mediante 3 programas

- **Entrenamiento en el puesto:** La Dirección asigna a un Supervisor o Jefe o Empleado especial un contenido establecido de lo que debe explicar y enseñar a hacer en un puesto específico de trabajo, generalmente a un reducido número de aprendices.

Es necesario que estos entrenadores conozcan las técnicas de guía y demostración y sepan formular objetivos sobre las destrezas que deben adquirirse y hacia donde puede moverse el empleado una vez terminado el evento.

- **Programa de rotación de puestos:** Con el fin de familiarizar a los empleados en diferentes áreas de operaciones, por intervalos se les cambia de puesto y de esta forma se logra un entrenamiento cruzado que sirve además para evaluar las capacidades del empleado para desempeñar adecuadamente ese nuevo cargo. la empresa podrá organizar rotación de puestos de 2 maneras:

Formalmente: ordenándolo para grupos específicos de empleados.

Informalmente: efectuando movimientos temporales pero cuidadosamente registrados con empleados que ven en este movimiento un incremento de habilidades para lograr futuras metas de carrera.

- **Programas de proyectos especiales:** Consiste en que individuos o grupos toman proyectos temporales fuera de su rutina normal de trabajo. Estos proyectos son relativamente fáciles de iniciar sin una política formal de la empresa y sin asignación de presupuesto especial.

Los resultados de este programa benefician a la empresa porque, por lo general, presentan diagnósticos desde puntos de vista diferentes y además benefician al empleado puesto que gana acceso a información

y conocimientos, especialmente si se realiza con equipos interdepartamentales.

3. Modalidad de Capacitación basada en Asesores y Guías

Esta modalidad incluye aquellos patrocinios formales o informales por parte de la empresa que animan a los empleados a participar en grupos donde se comparten experiencias y conocimientos laborales, tales como organizaciones profesionales, círculos de estudio laboral (muy utilizados actualmente en el Japón) y relaciones con guías o tutores.

La empresa requiere establecer sistemas para el aprendizaje informal y los participantes deben recibir alguna asistencia para reconocer estos recursos.

- Programa de Tutoría

El tutor aconseja al empleado sobre lo que contribuye al logro de sus metas. El sistema de tutores puede ser formal o informal. El primero estaría representado por tutores en planta designados por la Dirección para asesorar a tal o cual individuo en tal o cual trabajo de planta. El sistema formal de tutores estará constituido por los profesionales de la empresa.

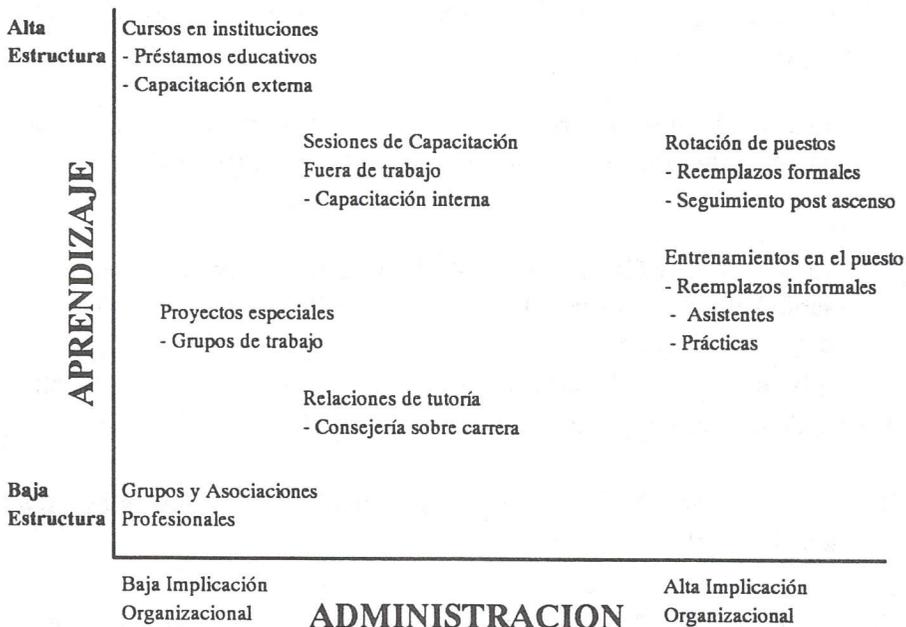
- Programa de pertenencia a Grupos o Asociaciones

Muchas organizaciones financian la participación de sus empleados en asociaciones o grupos profesionales, los cuales se dirigen al aprendizaje y desarrollo de sus miembros.

Estas asociaciones son buenos recursos para intercambiar ideas y suministrar ejemplos de cómo las tareas y los problemas se abordan en diferentes contextos.

4. Estructuración e implicación organizacional de los programas

Las modalidades de educación que ofrece la empresa, analizadas anteriormente ofrecen varios grados de estructuración y de implicación por parte de la organización que los empleados deben conocer en el momento de seleccionarlas. En el siguiente cuadro se presentan estas modalidades:



5. Areas responsables en los programas de capacitación

- **Alta Administración:** Es responsable por las decisiones políticas sobre programas de desarrollo de carrera, acuerdos sobre recursos de la organización, oportunidades que deben ser presentadas.

- **Profesionales de Capacitación y Recursos Humanos:** Son responsables del suministro de información, herramientas y guías que capacitan a los empleados para planificar e implementar su desarrollo y además son responsables de actuar como enlace con la alta administración.
- **Jefes y Supervisores Inmediatos:** Son responsables de suministrar el soporte y consejería primarios a los empleados para ayudarles a determinar sus opciones y actuar como enlace con los profesionales de recursos humanos para planear objetivos y evaluar los resultados de la capacitación en sus subalternos.
- **Los Empleados:** Son responsables de iniciar su propio desarrollo de carrera, tomar la capacitación requerida y aplicar en el trabajo lo adquirido.
- **La Unidad de Capacitación:** Es importante determinar las responsabilidades de esta Unidad, pues se concretan dentro de un sistema de desarrollo de carrera.

La Unidad de Capacitación debe definir e inventar las opciones de desarrollo de acuerdo con las necesidades y metas de los empleados.

Debe suministrar información y guía para que los empleados elijan los recursos disponibles.

Debe establecer sistemas de seguimiento de los resultados de la capacitación y utilización de las nuevas habilidades adquiridas.

Debe actualizar a los tutores así como a los jefes y supervisores en cuanto a opciones y metodología de desarrollo para facilitarles su función de coordinación y guía.

Debe velar porque los empleados participen en su propio desarrollo de carrera haciéndose cargo de sus propios planes y acciones.

La siguiente figura ilustra los roles de la Unidad de Capacitación, los de los participantes y los de otras personas en la organización en cuanto a programas de desarrollo de carrera y capacitación.

RESPONSABILIDADES DE LA UNIDAD DE CAPACITACION

CON LOS PARTICIPANTES EN DESARROLLO DE CARRERA

- Analizar necesidades
- Orientar programas
- Consejería
- Facilitar planeación y decisión sobre metas
- Seguimiento del Progreso
- Sugerir que opciones y recursos se pueden emplear
- Sugerir alternativas de movimiento ocupacional del empleado.

CON OTROS

- Obtener recursos
- Asesorar a jefes en habilidades de Consejería
- Revisar las alternativas de desarrollo que existen
- Establecer sistemas de monitoría
- Informar a la alta dirección
- Sugerir como utilizar los resultados de desarrollo de carrera
- Evaluar el retorno de la inversión

- Obtención de acuerdos sobre los programas
- Suministrar información sobre los programas

6. Retorno de la Inversión en Capacitación

La medición de algunas inversiones en recursos humanos es difícil, sin embargo, cuando la capacitación se enmarca dentro del desarrollo de carrera, probablemente se acrecientan las oportunidades de retorno favorable de la inversión sobre la capacitación.

El retorno de la inversión se mide así:

- **Orientado hacia utilidades.** Consiste en comparar los cambios en las utilidades de la compañía con los cambios en gastos de personal (incluyendo los costos de capacitación). Si las ganancias crecen en proporción mayor que los gastos en un período, los programas de capacitación y desarrollo de carrera son exitosos.

Sin embargo, debido a la complejidad de variables que operan en ese período es difícil ligar los cambios en utilidades estrictamente con la capacitación.

- **Orientado hacia cambios humanos.** Consiste en evaluar los cambios en áreas que probablemente están influenciadas por la capacitación, como reducción del número de reemplazos, evaluación del desempeño y reducción de quejas sobre el personal.
- **Orientados hacia el tiempo.** Consiste en evaluar los costos del tiempo empleado antes de un programa de capacitación y después de él, en aspectos tales como tiempo gastado en encontrar nuevos empleados para nuevos puestos, tiempo gastado debido a rotación etc.
- **Orientado hacia seguimiento.** Consiste en evaluar los resultados comportamentales, laborales del capacitado en cuanto al desempeño del trabajo mismo, metas individuales, planes de progreso y potencial para movimiento según las necesidades de la empresa.

Mientras más tiempo se gaste en planear y seleccionar eventos de Capacitación, dentro de un sistema de desarrollo de carrera, ésta será más efectiva en costos y los empleados, profesionales de Recursos Humanos y Directivos, obtendrán los mejores resultados.

7. Programa de Inducción al Ingreso

Inducción al Área de Trabajo	Dar una información general del área al cual ingresa el funcionario, especificando sus objetivos, políticas, normas a funcionarios que la conforman con el fin de ubicarlo dentro de su área de trabajo.
Entrenamiento en el Puesto de Trabajo	Suministrar el entrenamiento necesario para el desempeño en el cargo Entrega formalmente al funcionario toda la información relacionada con las funciones y responsabilidades del cargo
Curso de Inducción	Brindar una información de la empresa en términos de su historia, objetivos y estructura organizacional y de los beneficios y responsabilidades frente a la institución.

IMPORTANCIA DE LA CAPACITACION EN LA VERIFICACION DE DOCUMENTOS VALOR

*Hugo Salazar Marciales**

INTRODUCCION

La necesidad de aumentar la protección de los documentos valor contra los intentos de Falsificación y/ o Adulteración, requiere permanentemente el desarrollo de materias primas y sistemas de impresión y de información cada vez más sofisticados. Igualmente, y como parte fundamental de la seguridad, es indispensable un ambiente físico controlado, y un personal idóneo y capacitado que permita verificar las seguridades integrales contenidas en el documento.

Es de todos conocido, que durante el proceso regular de formación primaria, secundaria y profesional ó técnica, el hombre recibe una serie de conocimientos que le permitirán desempeñarse durante su vida productiva laboral. La efectividad de su trabajo dependerá en gran parte de la **Inducción y Entrenamiento** adecuado que reciba por parte de la Empresa y de sus

* Director de Calidad y Desarrollo Técnico Carvajal S.A.

compañeros de trabajo. Su futuro dependerá de su honestidad, de la **Educación para el Desarrollo** que le ofrezca la Organización y de la capacidad de asimilación y compromiso del individuo.

La Inducción y el Entrenamiento son una parte importante de la **Capacitación** que ofrece la Empresa, tanto en Programas formales masivos e individuales, como en Programas no-formales específicos en su sitio de trabajo o relacionados con el mismo. Esta capacitación no está orientada a recibir únicamente conocimientos, más bien tiene como objetivo el **mejoramiento continuo del desempeño**, lo cual es parte integral y esencial de la **Calidad Total**, proceso indispensable para la supervivencia y el desarrollo y en el cual deben estar todas las Organizaciones.

Los **documentos valor** del Sector Financiero, tales como cheques, certificados, bonos, entre otros, son impresos con características especiales que permiten, como se mencionó anteriormente, dificultar la acción de los delincuentes en intentos de Adulteraciones y/o Falsificaciones, pero para poder en verdad frustrar dichos intentos, los funcionarios encargados de visar o autorizar el trámite o pago de los mismos, deben tener no sólo el conocimiento de las seguridades incluidas en dichos documentos, sino la capacidad y la habilidad para verificarlas; por ello es indispensable capacitar efectivamente a todas y cada una de las personas que en una u otra forma tienen que ver con las mencionadas transacciones, entre ellas, Gerentes, Secretarios, Cajeros, Visadores, Contralores y Jefes de Seguridad.

En esencia, todos tenemos un enemigo común que es el Delincuente, por lo tanto, proveedores de insumos, impresores, sector financiero, clientes, usuarios y entidades relacionadas con éstos temas, debemos formar un frente coordinado contra él, en la medida de nuestras responsabilidades; si conocemos y ponemos en práctica las especificaciones y procedimientos acordados entre las partes, los niveles de riesgo disminuyen en alto grado, trayendo como consecuencia una mayor confianza en el Sector y en sus productos y

servicios y por lo tanto mayores beneficios sociales y económicos para las organizaciones.

CONCEPTOS GENERALES

Con el fin de facilitar la comunicación, se resumen algunos conceptos utilizados en el Sector con relación a la Seguridad de Documentos Valor:

Seguridad: Es la técnica de previsión y control de un riesgo, ya sea contra personas, instituciones o cosas.

Falsificación: Imitación de un objeto y/o transmisión original con materiales y/o procesos diferentes a los utilizados para elaborar el auténtico.

Adulteración: Modificación de cualquier parte de un objeto y/o transmisión original.

Condición Insegura: Cuando faltan elementos indispensables para que el objeto o la transmisión sea segura.

Acto Inseguro: Cuando no se verifican las seguridades y/o requisitos del objeto y/o transmisión.

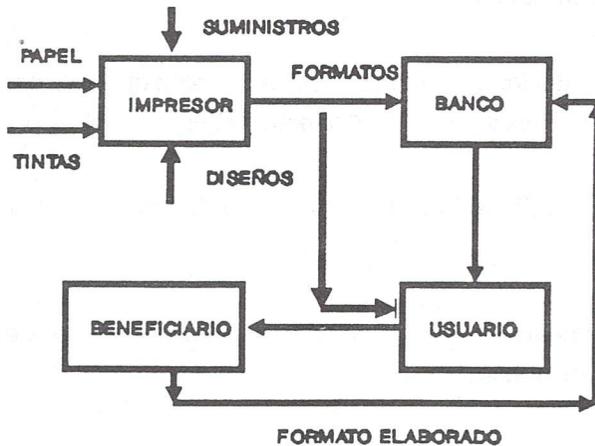
Protección: Es la técnica de interponer elementos para aislar, retardar y/o disminuir acciones inseguras tales como las adulteraciones y las falsificaciones.

Prevención: Es la técnica tendiente a garantizar la seguridad.

EL PROCESO DE PRODUCCION DE DOCUMENTOS VALOR

El siguiente diagrama explica en forma resumida, las principales etapas por las cuales pasa la elaboración un documento valor, en éste ejemplo, un cheque o un certificado. En cada una de éstas etapas se le agregan seguridades y son todas ellas en conjunto las que conforman la seguridad del documento y es al final del proceso donde se deben verificar su presencia inalterada para así hacerlo efectivo.

PROCESO DE PRODUCCION DE DOCUMENTOS VALOR



PROCESO DE CAPACITACION

Un proceso de capacitación pasa esencialmente por las siguientes fases:

Planeación: Cuando se debe definir el propósito específico de la Capacitación, su contenido, su metodología, su forma de evaluar, el sitio, la fecha, la hora y duración, los participantes, las ayudas prácticas, herramientas necesarias y los sistemas de seguimiento.

Ejecución: Realmente es la realización del proceso, el cual debe cumplir los propósitos y requerimientos indicados en la fase de planeación. Los participantes, entre los cuales se incluyen los instructores, realizan el programa propuesto. Esta fase debe ser lo más práctica posible, ilustrándose con casos reales.

Verificación: No sólo del proceso de capacitación, sino el desempeño de los participantes después de recibida la capacitación, deben llevarse registros estadísticos de la efectiva labor realizada y se deben realizar auditorías del proceso.

Mejoramiento: Periódicamente, al menos dos veces por año se debe revisar el proceso para actuar, ya sea para corregir o para mejorar el proceso.



LAS SEGURIDADES (Qué son, cómo se verifican, Qué Protegen?)

Básicamente, el proceso de capacitación se debe orientar en la forma más práctica posible, simulando la forma como el funcionario recibe el documento objeto de verificación, es por ello que se han clasificado las seguridades en los siguientes grupos, independiente de su origen:

Seguridades a simple vista: Son aquellas que se distinguen a simple vista sin necesidad de herramientas o sistemas especiales; tales como los diseños, la marca de agua, la penetrabilidad de las tintas, las claves impresas sobre los lotes de producción.

Seguridades con luces especiales: Son aquellas que requieren una iluminación especial para verificar su presencia.

Principalmente se incluyen las seguridades que requieren la necesidad de la luz ultravioleta para detectar su presencia e inalterabilidad, tales como los blanqueadores ópticos, las tintas fluorescentes, las fibrillas e impresiones especiales.

También se incluyen aquellas seguridades que requieren otro tipo de iluminación especial para su detección.

Seguridades químicas: Son aquellas que requieren de reactivos químicos especiales para detectar su presencia. Indican alguna manifestación visual, como cambio de color o forma, las más conocidas son reacciones a oxidantes clorados, reacciones solventes, reacciones acuosas, reacciones graso. En éstas se incluyen la reacción llamada nulo, la sensibilización a solventes, los sangrados, entre otros.

Seguridades micros: Son las que requieren lentes de aumento para su verificación, están incluidas las microlíneas, los fondos, los microtextos, etc.

Otras seguridades: En algunos casos se incluyen otras seguridades que se deben verificar mediante instrumentos especiales, como filtros, cabezas magnéticas, fotointerpretores o fotocopiadoras, etc.

CONCLUSION

En conclusión, la Capacitación es una de los medios más efectivos para disminuir los riesgos de estafas al Sector Financiero y Comercial, incluso se puede extender a los usuarios de los medios de pago, tales como el Comercio y la Industria. Del interés y el compromiso efectivo de las instituciones involucradas depende el éxito de su implementación.

ADMINISTRACION DEL RIESGO EN EL SECTOR FINANCIERO

*Ernesto Clavijo Salgado**

PROBLEMA CRECIENTE

- a) La situación actual señala una explosión de criminalidad; como ejemplos se tienen quiebras de bancos (USA, UK, Hong Kong, CCCI.)
- b) No todos los fraudes pueden prevenirse o evitarse
- c) La creciente siniestralidad ha venido obligando a un permanente incremento de primas
- d) De ordinario se generan dificultades por interpretación:
 - Lugar de la Pérdida
 - "Empleado"
 - "Falsa pretensión", "Aceptaciones"

Se destaca, como ejemplarizante sobre interpretación, el caso del Security Pacific Nat. Bank, pérdida iniciada por una llamada telefónica fuera del Banco

* Gerente Zabac Ajustadores.

(US\$ 10.200.000), donde se discutió largamente sobre el lugar de ocurrencia del dolo.

Definición de "Riesgos"

El problema con el fraude para la mayoría de las víctimas potenciales es no saber que serán golpeadas, ni en qué forma o cuantía. Es un hecho que todas las organizaciones son afectadas por el fraude, aunque el nivel sea desconocido.

Alrededor del mundo los niveles de culpabilidad de Directores y Funcionarios son variables; en USA son los más astringentes y tienden a serlo más. En UK, se requiere prueba de culpabilidad o de gran negligencia, para imponer obligaciones a un Director: "un director es obligado a ejercitar el cuidado de una persona de su mismo conocimiento y experiencia"; puede no obstante, sanear las fallas por rectificación, a menos que estas ocurran por:

- a) Conducta fraudulenta
- b) Actos que afecten en extremo a la empresa
- c) Fallas de deberes que lesionen los derechos de accionistas
- d) Fraudes contra accionistas minoritarios.

En USA, un director es indefectiblemente responsable por actos contra:

- La corporación
- Los accionistas
- La dirección de la corporación
- Los depositantes

- El fondo de depósitos de los seguros.

En USA un director es **"requerido para desarrollar sus deberes con el mismo cuidado, que hubiera tenido una prudente persona en la misma posición y bajo las mismas circunstancias."** Se tendrán en cuenta, los siguientes deberes:

1. Lealtad en extremo
2. Sus acciones deben basarse en razonable credibilidad
3. Sus acciones encaminadas en los mejores intereses de la empresa
4. Debe actuar con vigilancia y diligencia
5. No debe usar su posición para obtener ganancias personales, ni tampoco:
 - a) Asentir o fallar en prevenir repetidas violaciones a normas
 - b) Asentir o no impedir concesión de transacciones riesgosas (préstamos, concentración de crédito, debilidad de codeudores, sobregiros riesgosos);
 - c) No auditar operaciones
 - d) Asentir o no impedir prácticas de inversiones improvidentes
 - e) Fallar en prácticas de control interno.

"El mejor esquema de seguridad es la prudencia", por lo cual la prevención del fraude significa que los directores y la Administración:

- a) Harán esfuerzos para identificar y cuantificar los riesgos

- b) Fijarán objetivos de protección y establecerán y documentarán estrategias de control de riesgos
- c) Crearán políticas y destinarán recursos para implementar tales controles
- d) Desarrollarán efectivos controles, commensurables con los riesgos en-vueltos
- e) Vigilarán los resultados y apoyarán su cumplimiento
- f) Investigarán los casos de fraude y adelantarán todos los pasos neces-arios para recobrar las pérdidas.

LA NATURALEZA DE LOS RIESGOS

Se define bajo dos vertientes:

1. Probabilidad
2. Severidad

La "escala de importancia", basada en la expectativa anual (pérdida anual estimada) ALE, se determina por la siguiente fórmula:

$$\text{ALE} = \text{Probabilidad} \times \text{Severidad}$$

FRAUDE

Se entiende como la conducta deliberada contra una compañía o individuo, para obtener una ganancia deshonesta; puede cometerse contra:

Patrono
Empleados
Usuarios
Terceros
Gobierno

Conviene, para los efectos del Seguro de Bancos y responsabilidades, conocer la diferencia entre Crimen (violación de Ley Criminal) y dolo, por cuanto:

- a) La Policía actúa de oficio en cuanto a persecución del crimen, pero no puede hacerlo en caso de dolo, si la víctima no utiliza el medio de denunciar.
- b) Por regla general, se considera que pérdidas por fraude están entre el 2% y el 5% de los ingresos brutos de las empresas y que un elevado porcentaje (50 o más) del personal, considera la posibilidad de actuar fraudulentamente. Muchas de éstas pérdidas quedan sin persecución penal.

Motivaciones para el Fraude

a) Contra la Empresa

Los empleados de "cuello blanco", directores y gerentes; generalmente justifican su deshonestidad:

- Por envidia o resentimiento del éxito de otros empleados y de la empresa que los contrató
- Por una irreal y alta expectativa personal de ingresos económicos y reconocimientos
- Por desprecio hacia los sentimientos de otros y frecuentemente con irrespeto de sus superiores

- Por egoísmo y egocentrismo, con alegado impulso de circunstancias por encima de su control.

Los operadores de "cuello azul", generalmente llegan al fraude para "mejorar sus ingresos"; razonan que el empleo acepta "ciertos ganadores" y minimizan la importancia del dolo. Algunos aceptan la actitud de sus compañeros, por lo cual el fraude puede ser cometido por secciones enteras de una empresa.

b) Fraudes en interés de la empresa

Contra usuarios, Gobierno, proveedores; no envuelven ganancia personal, sino anhelo de promoción, especialmente si la empresa se encuentra en una etapa de declinación.

c) Criminales organizados

Se ha generalizado el dolo por la benevolencia de las penas legales; la motivación es solo la ganancia personal, que equipos humanos orientan y realizan, utilizando medios tecnificados.

d) Técnicos de Computación

El dolo por computación es generalmente cometido por jóvenes de gran preparación, en especial donde los jefes pertenecen a la generación de pre-computador, pues sus vacíos técnicos no les permite auscultar la configuración de actos dolosos.

e) Otras Motivaciones

Podrían existir influencias financieras o sociales (por fuera del trabajo), pero la cultura dentro de la empresa es muy importante. Hay una cercana correlación entre los niveles éticos y el estilo de gerencia de la empresa, la

eficiencia de sus controles y la escala y frecuencia de los fraudes (debilidad de la víctima), que pronto es percibida por el personal (participación pasiva de Gerencia).

Bases de la motivación:

- a) Incertidumbre económica y política
- b) Expectativa de inestabilidad personal
- c) Actitud indiferente o abusiva hacia la propiedad de otros
- d) Los criminólogos predicen para el futuro inmediato:
 - Aumento de fraudes por grupos organizados
 - Extorsión, más desarrollada y extendida a nuevos ámbitos
 - Convenio entre directores y personal de computación, más generalizada
 - Piratería (sabotaje)
 - Falsificación, apoyada en mecanismos de mayor sofisticación.

Teorías de la esencia del Fraude

El fraude se origina y fomenta en la combinación de oportunidad y motivación personal. La oportunidad generalmente depende de 3 factores:

- a) Acceso (cuentas, registros, sistemas)
- b) Conocimiento/práctica (para identificar y explotar la oportunidad)
- c) Tiempo (para planear y ejecutar el fraude)

Debe tomarse como cierto, que a mayor edad del patrono, mayores son las oportunidades de los empleados para cometer Fraude; a mayor especialización para cometimiento del Fraude, menor número de personas ordinariamente se compromete.

Estructuras de Seguridad

La fundamental estructura de Seguridad se apoya en su Sistema Gerencial basada en un alto nivel de Códigos, lo que podría ser comparable a un sistema convencional de "cerradura".

El sistema debe ser responsable de garantizar el control de acceso a usuarios, de asegurar apropiada ubicación de los códigos, generalmente en sometimiento de una tabla de autoridades, que puede aplicarse por individuos o por grupos, donde se fijan los privilegios y de impedir que suplantadores puedan penetrar dolosamente.

La tabla de autoridades tiene un directorio o diccionario, que comprueba que la actividad está permitida para el usuario. En Software se registran las operaciones diarias y se cargan a límites de consumo (saturación). El acceso doloso puede ser Activo o Pasivo.

- a) **Activo:** Trabajo deliberado de penetración (alta preparación)
- b) **Pasivo:** Encuentro de los detalles necesarios para vulnerar la seguridad (muchos casos se dan para individuos de mediana preparación).
El ingreso Pasivo se facilita por:
 - Informaciones en Directorios Internos
 - Identificación mediante sistemas de autodiscado, que con repetidos ensayos permitan descubrir el tono generado por un computador
 - Falta de cuidado (celo) de empleados

-
- Cuentas de teléfonos, no manejadas con seguridad
 - Llamadas de suplantación a usuarios (como "auditores"...)
 - Sobornos a empleados de la compañía, guardias de seguridad, personal de aseo, empleados de empresa de teléfonos.

Entre comunes fallas se encuentran usuarios, que por pereza o descuido, no cambian los archivos y los nombres de programas dados por el fabricante o instalador del computador, los cuales generalmente aparecen impresos en manuales. En algunas ocasiones se descubren informaciones en papeles carbón dentro de cestas de desperdicios.

El Fraude puede cometerse en forma sistemática (de más difícil descubrimiento) o en una sola ocasión (de manera violenta); puede concluir en:

- a) Sustracción de ingresos
- b) Sustracción de pagos.

El Fraude por Computador

La mayoría de los fraudes por computador se relacionan con aplicaciones financieras y son sistemáticos, antes que de una sola ocasión; la posición, sin embargo, ha sido cambiante por el crecimiento del sistema hacia la transferencia de fondos, procesos de control, inteligencia artificial e informática, con mayores exposiciones a pérdida como resultado tangible.

El Fraude por Computador debe ser examinado en 3 fases:

- a) Medio de entrada Acceso de (criminales) defraudadores
- b) Manipulación Facilitación o contribución de criminales

c) Conversión Conocimientos y experiencia

Acceso

Con autorización Abuso de Confianza

Con manipulación Mucha experiencia o inadecuada seguridad

Las oportunidades de acceso pueden ser difícilmente impedidas (o imposible), pues son de movimientos imperceptibles y se sujetan a una tenue línea divisoria entre comportamiento honesto y deshonesto, sólo es vulnerada por la motivación.

En algunos casos los defraudadores logran infiltrarse en empresas a través de aplicaciones de empleo.

Se considera que el Fraude puede restringirse:

1. Por comprobación de antecedentes, antes de otorgar algún privilegio de acceso.
2. Fijando limitación a autorizaciones para usuarios
3. Por reforzamiento de controles y detecciones oportunas.

Desafortunadamente debe confrontarse al Fraude Externo, que se comete mediante acción de personas de alta calificación técnica, y que para la empresa no tiene control directo alguno.

Acceso a través de conocimiento

1. En "Sistemas abiertos", por el manejo doloso de puertos de discado

2. Por claves (códigos) no manejados en forma segura
3. Por abuso de altos privilegios a usuarios.

El acceso a los sistemas exige una correcta comunicación e ingreso del código (contraseña), dentro del proceso, pueden generarse desviaciones:

- El usuario remoto, que intenta defraudar, carga su micro con un sistema de discado dentro de un programa de comunicaciones
 - Selecciona las opciones del menú
 - Disca el número telefónico, o el packet switch stream (PSS) y espera el tono de conexión del computador, "objetivo"
 - Conecta su micro colocando la bocina telefónica en un Par Acústico y opera el botón de "Retorno" de su computador; la pantalla aparece negra, mientras él debe responder a una serie de mensajes:
- * Clase de entrada
 - * Nombre del Programa
 - * Terminal (tipo)
 - * Cuenta
 - * Código (contraseña)
- Si comete algún error, la pantalla puede emitir señal de "emergencia".
 - Una vez ganado el acceso, él puede recibir "ayudas" y "menús", preguntándole puede seleccionar las opciones, archivos y programas requeridos.

- Se necesitan 3 piezas de información:
- Número telefónico del puerto de discado (PCS # identificación)
- La cuenta (Programa o Archivo)
- Apropiada contraseña (Código).

VIAS DE LA VULNERABILIDAD

Negligencia de Usuarios

En ocasiones, los usuarios son descuidados con el celo de sus códigos y los anotan en diarios, tarjetas, bades, directorios telefónicos, etc.

Además, con cierta frecuencia escogen Códigos (contraseñas) relacionadas con su actividad:

10% Asociados con sus nombres

5% Son caracteres simples (A, B,..)

8% Caracteres dobles (AA, aa,..)

12% Nombres comunes.

Como descuido generalizado está el no cambiar los Códigos al retiro de empleados privilegiados.

Penetradores

- a) Se utilizan micros para crear circunvalación de una cuenta o archivo conocidos, en base a que algunas contraseñas tendrán sólo 3 a 4 caracteres. Se intentan combinaciones de letras (A -Z), se ha comprobado como suficiente un tiempo aproximado de 2 meses x 24 horas al día, para obtener resultados en combinación de contraseñas hasta de

6 caracteres. Es posible que los computadores más avanzados puedan detectar los intentos de violación.

- b) En algunas ocasiones las contraseñas tienen el mismo nombre de los propietarios (el acierto se acerca al 5%).
- c) **Pequeños Genios.** El penetrador realiza un examen de nombres y considera que el usuario habrá de asociar la contraseña con su actividad; interiormente lo califica como una persona de inferiores niveles intelectuales a él.

Un caso típico fue el de una Cervecería en Estados Unidos, contra la cual el "pequeño genio" descubrió la contraseña "Beer". Ejemplo de penetración a industria láctea, podría ser:

Nombre de la Cuenta	Suposición de Correlación
Campo	Vaca
	Pasto
	Verde

d) **Penetradores con Intercepción y Engaño**

La técnica es particularmente exitosa para "quebrar" contraseñas y nombres de cuentas con base a informaciones públicas y sobre ciertos sistemas de correo bancario; los penetradores investigan en los sistemas de correo y establecen el formato que un usuario genuino esperaría ver durante la operación.

Programa su micro para reproducir el formato y para generar los mensajes normales de operación del Sistema del Computador Central; luego conecta su computador a la línea del teléfono, y desde otro teléfono marca a un genuino usuario; haciéndose pasar por "un ingeniero que está probando el sistema",

pregunta al usuario si desea marcar un número (el del teléfono controlado por el penetrador), con lo cual su micro logra captar el código y nombre de la cuenta. El penetrador vuelve a llamar al usuario para decirle que la prueba no fue satisfactoria, por lo cual deberá seguir utilizando su antiguo código.

e) Penetración por Falla en la Desconexión

Si el usuario falla en hacer desconexión después de una sesión autorizada, la línea al computador y hacia los archivos utilizados puede permanecer abierta.

El penetrador hace repetidos intentos hasta hallar la situación antes descrita, y cuando se encuentra conectado en esta forma, puede crear nuevas cuentas, otorgarse privilegios y códigos.

En una variación más sofisticada de este método, el penetrador, que ya ha encontrado una vía, es decir, una cuenta fallida en el computador "objetivo", escribe un programa de Engaño, para estimular el formato normal antes de la operación, el cual introduce pero no desconecta. El siguiente usuario genuino realiza la llamada y queda conectado con el Programa de Engaño, sobre el cual se puede captar el nombre de la cuenta y código. El usuario, al ser desconectado el Programa de Engaño, sólo cree que ha ocurrido una falla de comunicación.

f) Llamadas Dirigidas

El penetrador requiere a la compañía telefónica (en carta- membrete que ha sido sustraída de la empresa víctima) que durante los días festivos que siguen, las llamadas se hagan a otro número, el del penetrador, al cual está conectado su micro, que contiene un Programa de Engaño.

g) Conversaciones por el Computador

Algunos computadores aceptan comunicaciones de usuarios remotos, los cuales pueden conectar directamente al terminal y establecer conversaciones.

A través de una cuenta de bajo nivel en el computador de la víctima, en el cual previamente se ha escrito una falla simulada y un Programa de Engaño, el penetrador habla a un usuario genuino y recibe mensajes. Durante el curso de este diálogo, la línea de falla del Programa hace que la pantalla del usuario "quede en blanco", así que éste asumiría que ha tenido lugar una falla de comunicación. El Programa de Engaño entra en posesión y en la pantalla del usuario se restablece el formato. El usuario reingresa los datos de su cuenta y código, que son de inmediato capturados por el Programa de Engaño.

h) Computador Sobrecargado

En sistemas sobrecargados la demora en ejecutar instrucciones (particularmente en la búsqueda de Tablas de Autoridad), puede ser explotada. El penetrador escribe un Programa en una cuenta de bajo nivel en el computador de la víctima, para la cual ya ha obtenido acceso. Mientras él hace los intentos de acceso a dicha cuenta, aprovecha el tiempo de respuesta para hacer repetidos intentos en serie, al azar, en su computador remoto. Esto puede causar que el computador de la víctima entre en una falla y otorgue al penetrador un estatus de supervisoría. En este nivel el penetrador puede crear nuevas cuentas y leer códigos y archivos de alta seguridad.

i) Crédulos

Es un método "poco elegante" y no de la aceptación del penetrador calificado técnicamente. Esencialmente el penetrador (preferiblemente una bella mujer), con papeles preimpresos, espera a la salida de una empresa (que constituye su objetivo) e invita a la gente a contestar una encuesta, durante la cual puede obtener contraseñas (códigos) y otras informaciones.

Se han utilizado algunas variaciones al tema, como encuestas por correo, invitaciones a exhibiciones, encuentros con grupos de usuarios y demostraciones para ellos, todas las cuales dependen de la credibilidad de las víctimas potenciales.

j) Penetración por Sistemas de Respuesta

Los monitores de respuesta solicitan el servicio requerido de usuarios remotos, desconectan la línea y discan el número de un usuario autorizado. Algunos son poco seguros.

Por ejemplo, un penetrador puede programar su microcomputador al número al cual el equipo de monitoreo está conectado cada uno o dos segundos y cuando la comunicación ha quedado perfeccionada, generar el tono del discado normal que el sistema espera oír antes de llamar a un usuario genuino. El sistema es engañado al creer que tiene una línea "limpia", cuando en realidad está conectado con el computador del penetrador, desde el cual este gana acceso a los archivos que el usuario genuino está esperando en respuesta.

Aún más peligrosos son aquellos monitores de respuesta que como seguridad adicional utilizan líneas telefónicas separadas para realizar las llamadas de retorno. El penetrador repetidamente disca uno de estos números (usando las técnicas arriba descritas) y después de obtener conexión, solo debe esperar la respuesta del monitor; entonces corre un Programa de Engaño para el usuario conectado, quien creyendo que el computador lo está llamando, ingresa el nombre de su cuenta y el Código o contraseña, sin preguntar, lo cual es capturado por el penetrador.

k) Dominio Público y Virus Penetrantes

Operadores de Sistemas Comerciales, en la noche, pueden ser tentados a usar los equipos de la empresa para discar en los listados de los penetradores. Ellos pueden correr Programas y Juegos en los archivos de la empresa, lo cual puede ser desastroso. Estos Programas pueden contener virus, los cuales destruyen todos los archivos y compromete la seguridad. Hay penetradores dedicados a producir Programas virales.

l) Intercepción de Comunicaciones

Los impulsos enviados o recibidos por dos terminales del Computador pueden ser interceptados, con la misma facilidad que la intercepción telefónica: las señales transmitidas pueden ser grabadas a través de un radio-transmisor a una cinta y retransmitidas por un par a un terminal compatible o impresora. De este modo, todas las señales, incluida la Contraseña, pueden ser leídas. Alternativamente, equipos como un "datos-copio" (data-scope) pueden conectar en algún lugar de la línea, entre el computador del usuario remoto y el de la entidad.

Obviamente, cuando las señales se hacen a través de un sistema cerrado, las oportunidades de intercepción son restringidas a los puntos adyacentes de emisión o recepción. La encriptación aumenta las dificultades de violación.

m) Emanaciones

Los equipos de computación y las conexiones emanan ondas electromagnéticas y señales conductivas. Es posible interceptar y descifrar las emanaciones de un terminal con conocimientos especializados y práctica, utilizando un osciloscopio, cuyo costo es de aproximadamente US\$1.000.

n) Caballos de Troya

Resulta posible para un usuario con privilegios de bajo nivel, introducir un "Caballo de Troya" para vulnerar la seguridad en cuentas privilegiadas, programas o archivos.

Por ejemplo, un usuario de privilegios de bajo nivel escribe un programa de juegos en sus archivos y le dice al operador de la consola que él puede usarlos en sus ratos libres. El operador accesa estos juegos a través de la consola del sistema, donde se desarrollan los niveles de altos privilegios, desconociendo que el usuario ha escrito pequeñas rutinas en los programas de juegos, las

cuales, cuando son llamadas por el sistema, descargan todas las contraseñas de los niveles privilegiados en su archivo, para su futuro uso doloso; (este método requiere alta especialización).

o) Debilidades de la Operación

La operación de algunos sistemas presenta debilidades en los controles de seguridad, que permiten su violación o derivaciones. Por ejemplo, los Niveles de Privilegios son transportables a otros computadores del mismo tipo. Es posible así para un usuario introducir un programa fraudulento a un computador remoto y no protegido, usando el Sistema de Privilegios, que puede ser salvado en un diskette, el cual, cuando es cargado en el computador protegido, dará el Programa de Privilegios, permitiendo leer desde y escribir hacia los archivos protegidos.

Hay unos pocos sistemas con un alto nivel de seguridad; los mejores parecen ser el VMS, Versión 4 (Digital Equipment Corp), certificado en nivel C2, por el Departamento de Defensa de Estados Unidos.

p) Mantenimiento y Diagnósis

La seguridad puede ser vulnerada por ingenieros de mantenimiento, al sustituir componentes; por inhabilitación de los mecanismos de control; o por el uso de equipos de alto poder, en la diagnóstico de discos, que permiten leer los archivos protegidos.

Así mismo, presentan riesgo de exposición los sistemas donde se corren programas de diagnóstico en líneas remotas. Como un mínimo, todas las conexiones deberían ser hechas por los operadores, mientras todas las aplicaciones sensitivas y archivos de datos deberían ponerse fuera de línea antes de la rutina de diagnóstico.

Los diskettes que contienen los Programas usados por los ingenieros, deberían guardarse bajo extremas condiciones de seguridad.

q) Instalación y Diseño

Cuando se instalan o diseñan los Sistemas, pueden seleccionarse generalmente varias opciones, tales como los detalles sobre niveles que deban registrarse en los jornales de actividad. Esto puede comprometer la seguridad, si el usuario se atiene únicamente a las claves y contraseñas del diseño original.

r) Registros y Supresiones en la Consola

En algunos casos el acceso al Sistema puede ser alterado, si un perpetrador conscientemente ignora o fuerza los controles de seguridad a sabiendas de que él puede suprimir todas las trazas de su responsabilidad en los registros de actividad e informaciones de consola.

Los métodos de supresión de los registros varían de una máquina a otra, y pueden ser tan simples como la remoción de papel de la consola impresora, acomodaciones en programas, o al colocar un falso "finalizado" en los registros, incriminando detalles que no quedan impresos.

s) Degradación de Controles

Los controles pueden degradarse a tal extremo que los síntomas obvios de fraude o acceso ilegal sean pasados como errores. Por ejemplo, si el Programa de Control de Acceso puede ser acomodado para que niegue temporalmente acceso a usuarios genuinos, usuarios no autorizados contemporáneamente pueden ganar acceso.

t) Acceso a Través de Backups

Los backups de Archivos y Programas pueden proveer un efectivo medio para fraudes y rompimiento de la seguridad de las contraseñas. Los backups de Archivo pueden ser removidos de su lugar de almacenamiento, copiados, alterados y retornados a su sitio. El fraude puede lograrse cuando los Archivos y Programas sean cargados en la máquina; después del evento, el perpetrador y su método no son fácilmente detectables.

u) Facilidades (equipos)

Restringidas tales como Serperzap (IBM), Patch, Editor, etc., pueden ser usadas para lograr escapar a la acción de los controles a niveles de Directorio y facilitar así la lectura de contraseñas y direcciones. El mismo Programa puede ser usado para destruir o suprimir registros de su propio uso.

v) Panel de Operaciones

En adición a la consola normal del supervisor, algunos viejos y aún muy modernos computadores tienen interruptores de presión, por cuyo accionamiento pueden leerse datos o cambiarse en la memoria principal. En algunos sistemas es posible inhabilitar la cinta, disco o el impresor al accesar y cambiar el contenido del "control o registro de direcciones" en la memoria principal.

METODOS DE MANIPULACION

La manipulación de los Sistemas de Computación, se orienta de ordinario a obtener ganancia dolosa; para lograr los propósitos se apela a la creación de un falso crédito o débito en una de las cuentas (para posterior conversión) y su balance numérico.

Las vías de penetración dependen de la facilidad de la operación dentro de los procedimientos de rutina. Los principales métodos se anotan a continuación:

1. Falso Ingreso

1.1 Falsa Transacción:

El más común y fácil método de fraude consiste en la supresión o falseamiento de datos de transacciones previamente a la introducción al computador. El fraude puede ser cometido por una persona con apropiado nivel de acceso:

- a) Entrada adicional de datos (manipulación positiva)
- b) Omisión de entrada de datos válidos (manipulación negativa)
- c) Alteración de datos.

Los datos falsos son creados durante la etapa de preparación, con entrada manual, a través de Códigos o por otros medios automatizados. Usualmente, los más peligrosos fraudes envuelven manipulación negativa y son muy difíciles de detectar, porque generalmente escapan a las rutas de auditoría:

Método de Manipulación		
	Positiva	Negativa
Falsas compras	X	
Créditos en ventas	X	
Nómina	X	
Débitos en ventas		X
Devoluciones en compras		X
Gastos	X	
Ingresos por pagar	X	X

1.2 Alteración de los Códigos:

Los códigos de transacciones facultan al computador para identificar el tipo de operación que deba procesarse. La alteración del código facilita el fraude; los más vulnerables códigos son aquellos que:

- a) Permiten el movimiento de bienes sin débito a una cuenta personal
- b) Se refieren a aplicación de precios de mercancías
- c) Realizan ajuste de existencias sin cargo a una cuenta personal
- d) Facilitan transferencias entre dependencias o sucursales.

1.3 Forma de "Jineteo/ Turbina":

Se debita cuenta sana por Crédito hacia cuenta dolosa; pago del primer débito con un 2o. más elevado y abono del diferencial a la cuenta dolosa; continúa el ciclo.

1.4 Diferimiento y ocultamiento:

En algunos sistemas de cuentas, debido a la distancia entre pagador y cobrador, el crédito puede asignarse antes que el correspondiente débito sea llevado a la cuenta.

El sistema de fraude puede desarrollarse en una serie de cuentas, tanto internas como externas y puede envolver proveedores, usuarios o bancos.

Los fraudes de este tipo tienen una vida limitada y pueden concluir en una transferencia final hacia una cuenta inactiva o a Ganancias y Pérdidas.

1.5 Rechazo por error:

Ingresos, particularmente los anotados en cinta magnética o códigos de barras, pueden deliberadamente corromperse de tal modo que los datos no sean aceptados por el Computador. Cuando se rechazan se sitúan en una cuenta en suspenso o en un ciclo de espera para clarificación o corrección, de tal modo que quedan a disposición de una manipulación fraudulenta. Estos fraudes no afectan los registros de balance.

2. Manipulaciones de Egresos

El computador puede manipularse tanto para fraudes internos como externos.

2.1 Fraudes Internos:

2.1.1 Los egresos pueden ser destruidos u ocultados:

- a) Para desaparecer el impacto del fraude
- b) Para justificar cuentas subsidiarias sometidas a control (en el movimiento de cuentas personales que tengan balances crédito).

2.1.2 Los egresos pueden ser manipulados cuando:

- a) Se reprocesan o reimprimen salidas incriminadas (con destrucción de originales)
- b) Se detectan Archivos en línea esperando servicio de impresión.

2.1.3 Los egresos pueden ser duplicados por:

- a) Doble emisión de cheques (nómina u otros pagos masivos)
- b) Inflar valores de inventario de cierre fiscal.

Generalmente los menos significativos componentes del Sistema son las impresoras, donde quedan los documentos en línea para alimentación al sistema; pero allí precisamente pueden cursarse fácilmente las alternativas dolosas.

2.2 Fraudes Externos

Pueden perpetrarse por accionistas, usuarios, proveedores, bancos y auditores externos; de ordinario la colusión se produce entre gerentes, administradores, procesadores de datos, mediante los mecanismos de:

- a) Destrucción o supresión de egresos
- b) Manipulación
- c) Duplicación.

Con objetivo de:

- a) Reducir responsabilidades en operaciones externas
- b) Dar apariencia de mejoras de rendimientos.

2.3 Manipulación de Archivos Maestros

Los Archivos Maestros (en database o no) proveen medios fáciles de fraude; usualmente son el eslabón entre la fuente documentaria y los asientos formales de cuentas. Aunque los departamentos de usuarios pueden ejercer adecuados controles sobre las transacciones cumplidas, los Archivos Maestros son menos fáciles de salvaguardar, particularmente sobre la marcha o en el corto tiempo de encomiendas. Los Archivos más atractivos de manipulación, son:

MANIPULACION	
Item	Alterado por:
a) Nómina Nombre y Código de empleados Salarios Comisiones y Bonificaciones Impuestos sobre salarios	Gerentes y Secretarias Gerentes y Secretarias Jefes de Ventas Personal Operativo
b) Ventas Listas de precios Descuentos Direcciones de entrega Límite de créditos	Jefes de Ventas
c) Inventarios Listados Ajustes contables Pérdidas toleradas Códigos de productos	Jefes de Almacén

2.4 Explotación de excepciones

En la mayoría de las empresas los Sistemas de Computación registran el 80% o 90% de todas las transacciones. El resto, es llevado manualmente, bajo rutinas prefijadas, lo cual provee un campo fértil para el fraude. Ejemplo:

- a) Manejo de transacciones especiales

- b) Transferencias interbancarias
- c) Compras de bienes de capital
- d) Ajustes entre cuentas.

3. Cuentas Inactivas o en Suspenso

Frecuentemente algunas cuentas deben permanecer en suspenso mientras se aclaran errores; hacen parte de una doble entrada al sistema y son normalmente incluidas en el Balance de Prueba.

Las posibilidades de fraude surgen si los créditos que deberían ser dirigidos a una cuenta de suspenso son deliberadamente desviados a una cuenta personal, lo cual indudablemente abre ventajas para el propietario de la cuenta.

4. Uso Doloso de Facilidades Restringidas

Las facilidades restringidas son poderosas herramientas usadas por programadores para detectar fallas del Sistema, corregir asientos de balance, copiar y restaurar archivos y para asistir, en términos generales, a la depuración de las operaciones.

Estas herramientas son normalmente guardadas en diskettes colocados en línea del computador y son solicitadas por una apropiada contraseña. Cuando son retiradas del Sistema, pueden ser utilizadas bajo un diferente nombre, para uso ilícito.

Los mayores fabricantes de computadores proveen facilidades que pueden ser introducidas al Sistema o mantenidas en módulos separados:

Fabricante	Facilidades
IBM:	Data Interpile transfer, testing and operations Superzap Patch Data file utility Alter/display File dump and restore
DIGITAL	Patch Sus Editor Primer
PRIME	File utility Direct disk Editor Edit

5. Enmiendas a Programas

5.1. Los Programas pueden ser enmendados durante su creación y mientras se someten a mantenimiento o actualización; las enmiendas pueden cursarse en:

- a) Nombre y número de una cuenta de usuario
- b) Fecha de transacción
- c) Cantidad de bienes (mercancías..)
- d) Tipo de bienes

- e) Un asiento especial
- f) instrucciones sobre control de trabajo
- g) intervenciones del operador.

5.2. La rutina no autorizada o fraudulenta puede ser introducida en muchas partes de un Programa. Usualmente se acondiciona dolosamente para instrucciones importantes en una o más de las siguientes etapas:

a) Etapa de validación (débitos)

- Para rechazar datos válidos
- Para aceptar datos inválidos
- Para eludir control de balances
- Para desviar ítems entre cuentas, sin afectar el control de totales.

b) Etapa de procesamiento

- Desviaciones entre cuentas
- Mitigación o aumento de acumulaciones
- Archivos maestros referidos (especiales)
- Manipulaciones positivas
- Supresión de informaciones
- Falsos listados de prueba

-
- Excusas "justificadas" de manipulaciones.

c) Salidas (créditos)

- Supresión de impresiones
- Repetición de impresiones

Estos ejercicios dolosos producen aumento aparente de Activos o Supresión de responsabilidades. La programación de fraudes requiere alto nivel de especialización; en la mayoría de los casos, la conversión es un elemento de difícil manejo, excepto cuando se refiere a supresión de ventas o cuando está apoyada por colusión de usuarios.

6. Manipulación de las Instrucciones de Control del Trabajo (JCL)

El control de trabajo atiende al proceso de las aplicaciones de un computador: dice al computador qué programa, qué debe ejecutar, cuál dato leer, dónde escribir la transacción. ("JCL" es un lenguaje que interviene con la operación del sistema y automatiza una gran parte del trabajo de los operadores).

En muchos casos las instrucciones JCL se colocan en línea y pueden ser enmendadas para desviar el procesamiento a un programa fraudulento. Normalmente las primeras dos o tres instrucciones del JCL contienen el "Código de Cuentas", que puede ser falseado o cancelado en determinadas rutas (con inclusión de compilaciones adicionales del programa).

7. Explotación de la Debilidad de Operaciones

Resulta un éxito (fraudulento), el cambio en las operaciones del sistema, que exige de calificada especialización, cuidadoso planeamiento, control del proceso y tiempo. Los principales métodos son:

METODOS			
Cómo	A través de	Cuándo	Medio usado
Enmiendas en operación del sistema:	Proveedor	Instalación	?
Compilación	Empresa	Mantenimiento	Superzap
Rápidos descargos			
Restauración			
Entrada/salida			
Filmación	Software	Nueva emisión	Sustitución
Comunicaciones de medios			Cancelación
Archivo:			
Manejo del Archivo	Empresa	Cambio	falla de máquina
Manejo de micros			

Cada sistema presenta vías de acceso, algunas veces deliberadamente dolosas, pero frecuentemente por accidente, las cuales son extremadamente difíciles de identificar (los propios fabricantes admiten tales fallas).

CONVERSION

En esta etapa pueden generarse una gran cantidad de fraudes. Hay un gran número de posibilidades, como:

1. Conversión de mercancías sustraídas

La manipulación de cuentas puede ser convertida en liberación de mercancías para el perpetrador, o más comúnmente hacia un "receptor" con quien el empleado está en colusión, quienes se ajustan al siguiente perfil:

-
- Personas dedicadas al cambio de moneda, en bajos niveles
 - Propietarios solos de un negocio
 - Negocios con historia de quiebras
 - Negocios de alto movimiento, que coloquen órdenes por pequeñas sumas (indicaría limitaciones de caja)
 - Fraudes en créditos de Compañía "fronting"
 - Comerciantes itinerantes
 - Negocios con dificultades presentes.

El "lavado" de mercancías se cubre por facturas, falsas o genuinas, aunque estas últimas podrían tener una tramitación de origen doloso. Cuando las facturas de la empresa víctima no correspondan a la realidad, el dolo puede identificarse por:

- a) Menores precios
- b) Amplios rangos de mercancías, en pequeñas cantidades
- c) No compatibilidad (consistencia) con la clase de negocio del receptor.

2. Conversión de dineros recibidos

Esta es una de las conversiones de más difícil identificación para la víctima, porque tiene lugar fuera de su control; la conversión puede hacerse íntegramente en forma interna o con apoyo externo.

2.1 Conversión Interna

Se opera por cheques de ingreso, cuyos asientos omitidos de los Libros de Caja y de Cuentas Corrientes, son llevados directamente a la Cuenta de Bancos, para cubrir faltantes o para soportar futuros fraudes. Alternativamente los cheques pueden ser depositados en la cuenta bancaria de la víctima, pero sin registro en el Libro de Caja, pagos y Cuentas Corrientes con un falso origen. Este es el caso típico del "jineteo".

2.2 Conversión Externa

Cheques de Ingreso pueden ser sustraídos y convertidos fuera de los registros de la empresa víctima:

- a) Endosados y negociados a través de un tercero
- b) Nombre del beneficiario alterado y depositado en una cuenta ajena
- c) Robados y reemplazados por un cheque personal de menor valor
- d) Pagados a un banco no autorizado, a nombre de la empresa.

Los ingresos que pueden seleccionarse para este tipo de conversión, son generalmente los más difíciles de controlar, tales como:

- a) Avances de pagos
- b) Depósitos
- c) Deudas malas de dividendos
- d) Otros ingresos distintos de ventas.

2.3 Conversión de Cheques de Gastos

Los cheques de pagos o gastos pueden ser convertidos como resultado de previa manipulación en las cuentas a que se destinan. Son vulnerables a los siguientes métodos:

- Alteración del nombre de beneficiarios
- Depósito en cuentas no autorizadas de la propia empresa
- Endoso en favor de terceros
- Sustitución por otros cheques.

2.4 Conversión de transferencia electrónica de fondos

Las instrucciones de pago a distancia por vías computarizadas son vulnerables, particularmente en función del tiempo. Se añade a ello la gravedad creciente de los fraudes, cuando:

- a) Se altera el número de la cuenta del beneficiario
- b) Se realizan pagos adicionales sin afectar los tests
- c) Se alteran las instrucciones, diferentes en detalle y no en el total
- d) Se explotan incompatibilidades de cambio
- e) Se interceptan y alteran instrucciones por télex.

CONCLUSIONES SOBRE EL FRAUDE POR COMPUTACION

El fraude por computación, a pesar de su aparente complejidad, es predecible por las oportunidades de:

- a) Acceso
- b) Manipulación
- c) Conversión.

Aunque algunos casos, particularmente los de "una sola ocurrencia", como la Transmisión Electrónica de Fondos, que puede envolver graves pérdidas ("pérdidas debilitantes"), la mayoría son menos severos y pueden ser controlados.

TIPOS DE ALTO RIESGO DEL FRAUDE

Es claro que todas las empresas están expuestas al fraude por varios métodos y magnitudes, pero solo unas pocas llegan al nivel de resultados catastróficos.

Los tipos de fraude (tanto si son por computador como si no), que usualmente tienen un mayor impacto en la víctima, se enuncian a continuación:

FRAUDES			
Tipo de Fraude	Cometido por	Contra	Seguro
Alteración de informaciones	Propietarios, accionistas	Potenciales inversionistas Posibles compradores de la empresa	No

FRAUDES			
Tipo de Fraude	Cometido por	Contra	Seguro
Defraudación, Desfalco,	Empleados de ventas, publicidad en colusión con usuarios y proveedores	Empresa	Fidelidad
Defraudación,	Empleados, criminales organizados (una sola ocurrencia)	Usuarios de Transf. Elect. de Fondos principios Básicos)	Fidelidad o amparo de crimen electrón.
Conflictos de interés, soborno	Empleados: desviación en compras y ventas; utilización de los recursos de la empresa para propósitos personales	Empresa	Fidelidad
Defraudación	Empleados, en colusión con proveedores para compras infladas o con usuarios, en supresión de ventas	Empresa	Fidelidad
Engaño	Terceros, criminales organizados y oportunistas, al entregar productos falsificados o de baja calidad	Distribuidores	No

FRAUDES			
Tipo de Fraude	Cometido por	Contra	Seguro
Extorsión	Criminales organizados, quienes amenazan con envenenamiento de productos a cambio de rescate	Grandes Corporac.	No
Extorsión	Criminales organizados, quienes secuestran a funcionarios de bancos por pago de rescate	Bancos	Extorsión en B.B.B.
Piratería industrial	Competidores, quienes copian patentes y falsifican productos	Empresa	No
Espionaje Industrial	Competidores, a través de empleados desleales de la empresa, quienes entregan secretos industriales e investigaciones	Empresa	No
Defraudación	Empleados (Depto. Crédito) autorizados para realizar avances a terceros, generalmente bajo soborno	Empresa	Fidelidad

FRAUDES			
Tipo de Fraude	Cometido por	Contra	Seguro
Fraudes en inversiones y franquicias	Criminales organizados quienes llevan a inversionistas a invertir en Compañías ficticias, transacciones falsas (certificados falsos)	Inversionistas	No
Abuso de Confianza, defraudación	Choferes de servicio de entrega, quienes recortan los envíos	Empresa y usuarios	Fidelidad
Defraudación	Empleados, quienes cambian la ruta de transacciones en moneda extranjera, para tener beneficios de cambio, o el uso de fondos para mover un mercado en favor de interés particular. Hay restitución del dinero usado	Empresa	Usualmente no cubierta: para empresas industriales o comerciales, pero amparada en Bancos
Abuso de Confianza	Empleados, al inflar los gastos de viaje	Empresa	Fidelidad

Responsabilidad de Directores

El Fraude es un serio y creciente problema, el cual, puede comprometer la responsabilidad de directores y funcionarios por alegada negligencia, fallas de dirección, fallas en actuar con prudencia y celo en el cuidado de bienes y capital. La Cobertura de Responsabilidad de Directores y Funcionarios D y O, puede satisfacer esta necesidad. La Cobertura no aplica defraudación por parte de directores y funcionarios.

POLIZAS DISPONIBLES

- a) U.K.: Sindicatos (respons. ilimitada) 90% del mercado. A partir de 1.993 tiende a fijar responsabilidad limitada, al cambiar el sistema social de Sindicatos por el de Corporaciones
- b) U.S.A.: Corporaciones (respons. limitada)

Los Corredores deben buscar dispersión en el Reaseguro.

Diferencias entre los mercados de UK y USA

- a) En UK, la parte perdedora en litigio reembolsa costas a la ganadora
- b) En USA, cada parte cubre sus costas de litigio. Por estos motivos, en USA los Reaseguradores están en mejor disposición de ir a Tribunales.

En USA los Aseguradores conforman un Comité, el Surety Ass. of America; en UK, el Bankers'Blanket Bond.

Mercado

Las Pólizas presentan importantes diferencias; p. ej, en Asia el Blanket Band solo ampara Infidelidad de Empleados; Hanc 83, de UK, fue diseñada en términos más generosos que la Forma 24, USA.

En los mercados poco sofisticados se busca:

- a) Limitar las coberturas
- b) Fijar primas hasta el máximo tolerable.

El solo hecho de tener Póliza Bancaria sin que se cubran todas las exposiciones, es malgastar el dinero. El seguro debe cubrir todas las exposiciones, política permanente.

Por presiones de mercado, algunas veces las Pólizas se encuentran como una serie de remiendos; en otros casos, se presenta cruce de amparos, y hasta en unos, carencia o vacío de coberturas. Algunas Pólizas presentan propias limitaciones de redacción (p. ej, cláusula 2 de Hanc 83 limita excesivamente el recobro de los costos de Contadores).

Preámbulo de las Pólizas

1. La Cobertura está condicionada a la exactitud de la solicitud, y algunas veces, a la correspondencia o informaciones suministradas por el Asegurado.
2. Debe determinarse si la cobertura se hace:
 - Sobre pérdidas ocurridas y/o descubiertas durante la vigencia
 - Bajo la Forma de Descubrimiento, con retroactividad que ha venido ocupando un lugar preferencial sobre la modalidad de "ocurrencia".

Cuadro de la Póliza

- Identifica al Asegurado, coberturas, primas y deducibles
- Establece si la Póliza responde:
 - a) Por términos de ocurrencia individual (con reinstalación automática)
 - b) Por límite agregado de Pérdidas. Responsabilidad máxima/año.

Cláusulas Generales de Amparo

Fidelidad	Falsificación o alteración
Locales	Seguridades
Tránsito	Moneda falsificada.

Convenios Generales

La Póliza puede extenderse:

- Por nombre de múltiples Beneficiarios
- Por noticia de: Empleados o funcionarios adicionales; consolidación, fusión o compra de activos; cambio de control.
- A Garantías
- Por Unión de Asegurados
- Por Costas legales u honorarios de abogados.

Definiciones

Aunque parezca una sección de la Póliza sin mayor importancia, de hecho, es vital en la interpretación de los mutuos compromisos. Por esto, cuando un término no está específicamente definido, el significado debe tomarse del Universal Commercial Code o del Blacks Dictionary.

Exclusiones

- Sección de la Póliza que fija límites de sus obligaciones
- Determina si la Póliza es de Descubrimiento u Ocurrencia
- Debe entenderse que aunque el listado de Exclusiones aplica totalmente, otras están escondidas dentro de las definiciones o son agregadas por endoso.

Límite de Responsabilidad

No es acumulativo año a año.

Descubrimiento de la Pérdida

Fija el límite de tiempo para dar aviso al Asegurador, fuera del cual el reclamo puede ser rechazado.

Valuación

Fija la metodología para calcular el monto de las pérdidas.

Salvamento, Recuperación, Subrogación

- Salvamento: el monto descarga su valor en la pérdida y se balancea con la indemnización, como lo determinan las condiciones específicas.

- Recuperación: Normalmente se aplica en este orden de prioridades:
 - a) Reembolsar al Asegurado por gastos de recuperación
 - b) Reembolsar al Asegurado, por el exceso de la pérdida sobre el monto de la Póliza
 - c) Reembolsar a la Compañía por el pago hecho al Asegurado, agotadas las sumas fijadas para a)y b).

Beneficios exclusivos y otros seguros

- a) La Póliza prohíbe extenderse a un liquidador, secuestre o a cualquier ente regulador que pueda controlar las operaciones del Asegurado
- b) En caso de otros seguros que concurran, la Póliza obra en exceso sobre las coberturas que sean comunes entre las varias Pólizas.

Cancelación

La Póliza puede cancelarse como un todo o para un empleado. Las condiciones usuales incluyen:

- Noticia escrita de la Compañía de Seguros
- Petición del Asegurado
- Liquidación del Asegurado
- Traslado de dominio o por fusión con otra institución.

En adición, se cancela automáticamente para un empleado al ser descubierta deshonestidad.

Cualquier reclamo fraudulento del Asegurado o en su nombre, anula la Póliza. En algunos casos, un reclamo exagerado (aún inocentemente presentado), puede poner el reclamo y la Póliza en cuestionamiento.

Derechos después de Cancelación

La Cobertura puede extenderse para dar aviso de pérdidas, después de extinguido el término de la Póliza. En ocasiones se cobra prima adicional.

Endosos

Se emiten para ampliar o reducir las coberturas.

ANALISIS DE LA POLIZA, BENEFICIOS PRACTICOS

1. Campo y Métodos de la Evaluación del Riesgo

1.1 Posición actual de los Aseguradores

Las Compañías de Seguros "alegadamente" confían en las solicitudes para determinar la base de cálculo de las primas. Insisten en la necesidad de identificar los riesgos, pero los estudios generalmente son superficiales, pues **carecen de análisis sobre estrategias de control.**

Hasta tanto una empresa comprenda la naturaleza y extensión de sus exposiciones de riesgo, no estará en capacidad de considerar si el seguro o cualquier otra forma de protección y control, son justificables o no.

Riesgos	Controles
Asegurado (necesidad de Protección)	Evaluación de Riesgos Determinación de estrategias
Corredor de Seguros (es interpelado) Recomendaciones	Definición de requerimientos Consulta a Corredor de Seguros Defensa de posición
Compra Póliza	Negociación Póliza Estudio Crítico de la Póliza

1.2 Método de acercamiento y fuentes de asistencia

Cada empresa debería hacer esfuerzos para catalogar y cuantificar los riesgos, especialmente aquellos que envuelven deshonestidad, manipulación por computador, errores y negligencia.

En la mayoría de los casos son consultados especialistas independientes, que determinan el riesgo en forma comprensiva, con las siguientes ventajas:

- a) Experiencia y manejo cuidadoso de las situaciones
- b) Rapidez y costo
- c) Mínima interrupción de las operaciones
- d) Habilidad de examinar las necesidades de seguro

- e) Independencia con Compañías y Corredores
- f) Independencia con Auditores y Revisores Fiscales.

La empresa prudentemente evaluará al Consultor, después de considerar los siguientes aspectos:

- a) Elaborar lista de consultores
- b) Explicar sus necesidades
- c) Entrevistar a los directivos de los consultores pre- elegidos
- d) Fijar puntaje, de acuerdo con atributos, en valores de 0 ("bajo") hasta 40, ("alto") y calificar el "peso" (según importancia tema)
- e) Discutir la propuesta con el más calificado.

La propuesta debe contener:

1. Recursos y especializaciones del Consultor
2. Detalles precisos de los servicios, indicando el método de acercamiento, presupuesto y tiempo
3. Nombres y calificaciones del personal asignado al trabajo
4. Nombres y direcciones de al menos dos clientes para quienes se haya cursado un trabajo similar

5. Detalles sobre potenciales conflictos de interés

6. Contrato escrito con las bases de la propuesta.

SELECCION DEL CONSULTOR						
Cualidades esenciales	Aceptación de Cualidades					
	A	B	C	D	E	F
Absoluta honestidad	x	x	x		x	
Impecables resultados	x	x	x		x	
Sanidad Financiera y existencia legal de la empresa	x		x	x	x	x
Record de trabajos similares	x		x			x
Independencia con Aseguradores, Corredores, Auditores	x	x	x		x	x
Especialidad en aspectos bajo revisión	x		x			x

Cuadro de Calificación				
Selección:	Consultor Satisface			
Atributos deseables		A	C	E
	Peso	Puntaje		
		0-20	0-20	0-20
Parámetros calificadorios Personal asignado, con récord sobre el mismo tipo de trabajo Calificación	50	20 (1000)	10 (500)	15 (750)
Parámetros calificadorios Récord de asignaciones	40	20	20	10

Cuadro de Calificación				
Selección:		Consultor Satisface		
Atributos deseables		A	C	E
	Peso		Puntaje	
		0-20	0-20	0-20
cumplidas en tiempo y dentro del proyecto asignado -- Calificación		(800)	(800)	(400)
Parámetros calificadorios Definidas políticas internas y ética en la conducción de sus negocios -- Calificación	40	10 (400)	5 (200)	10 (400)
Parámetros calificadorios Buena y clara estructuración de la propuesta -- Calificación	30	20 (600)	10 (300)	30 (900)
Parámetros calificadorios Acercamiento práctico y plan de trabajo	50	40 (2000)	20 (1000)	20 (1000)
Totales máximos (ideales)	(4800)+	(2800)+	(3.450)=	11.050

1.3 Análisis Interés de los Riesgos

Cuando una organización tenga recursos humanos y pueda asignar tiempo para llevar a cabo la evaluación de los riesgos, se recomienda que analice los siguientes pasos:

1.3.1. Escogencia del cuadro de trabajo

- Contador Jefe
- Jefe de Programación
- Auditor interno
- Jefe de Seguridad
- Representantes de Departamento de Usuarios
- Especialista de Computación
- Todos tendrán acceso a los niveles de Dirección.

1.3.2. Términos de Referencia

Deben ser preparados con toda precisión sobre el tema por la Gerencia, explicando los extremos de tiempo y límites de la intervención.

1.3.3 Identificación de los Riesgos

- a) En grandes Organizaciones deberían formarse " pequeñas Unidades Lógicas"
- b) En Procesamiento de Datos deben hacerse cuidadosos planeamientos debido a la dificultad de definir sus fronteras, las cuales deberían ser fijadas por el Cuadro Técnico.
- c) Deben ser considerados los riesgos según su especie en:
 - Accidentales
 - Naturales
 - Deliberados.
- d) Deben agruparse los riesgos según la Ocurrencia y participación:
 - Una sola ocurrencia
 - Ocurrencia sistemática (continua)

- Empleados que pueden participar
 - Personal externo que puede participar.
- e) Deben calificarse los riesgos de acuerdo con el impacto económico anual:
- Frecuencia
 - Severidad.

Fuentes de Información		
Naturaleza del Riesgo	Fuentes de Análisis	Desarrollo del Análisis
Accidental	Reportes Públicos Estadísticas internas	Análisis Subjetivo
Natural	Estadísticas de Aseguradores	Análisis Objetivo
Deliberado	Experiencia Previa	Análisis de Vulnerabilidad Experiencia Interna Informaciones externas.

1.3.4 Determinación de Frecuencia y Severidad

- a) **Frecuencia** (Probabilidad) debe "estimarse" para cada riesgo en rangos que varían entre 1 y 20 veces por año.
- b) **Severidad:** monto en valores económicos.
 $EAC \text{ (Estimated Annual Cost)} = F \times S$
 El costo de un incidente puede incluir:
- Pérdidas económicas directas

- Pérdidas consecuenciales, incluidas Pérdidas por Interrupción
- Pérdida de información confidencial
- Pérdida de recursos técnicos
- Exposición a riesgos por no cumplimiento de la operación del Sistema.

Frecuentemente el costo primo de un incidente es una fracción de la severidad, que puede aproximarse al quíntuplo o décuplo de aquel.

1.3.5 Estimados del EAC

Las hojas de análisis deben ser resumidas e ideadas por el Cuadro Técnico, bajo la previa creación de un "Catálogo de Riesgos", que se deriva de un estimado subjetivo. Este debe ser manejado con cuidado, como base para determinar la estrategia del Control y Evaluación de los Riesgos.

2. Decisiones en el Manejo de Riesgos

OPCIONES EN MANEJO DE RIESGOS		
Severidad	Frecuencia	
	Alta	Baja
Alta	Reducir los riesgos a través del mejoramiento de controles o cambios estratégicos. Considerar el Seguro y Planes de Contingencia.	Transferir a través del Seguro o de Planes de Contingencia. Controles adicionales podían no fijar una reducción del riesgo.
Baja	(Aceptar) Asumir estos riesgos, aunque se hacen necesario controles adicionales para reducir la frecuencia.	Asumir estos riesgos, pero evaluando previamente el Costo-Beneficio de Controles adicionales.

Algunos riesgos pueden reducirse, por ejemplo, si una o dos aplicaciones del Sistema sean críticas; convendría eliminar el acceso remoto o remover las aplicaciones a un computador menor, totalmente controlado.

Para Riesgos Catastróficos o Debilitantes, que no puedan ser reducidos o evitados, debe considerarse el Seguro como la principal alternativa.

3. Requerimientos de Seguros

La estrategia debe ser bien definida, pues la decisión debe darse entre comprar o no comprar Seguro (asumir riesgos).

4. Implementación y Mantenimiento de Controles

Corresponde a la actividad de la Gerencia implementar con debida urgencia los controles y fijar la logística para su preservación.

Debe hacerse una auditoría de los Controles, por lo menos una vez cada dos años, con introducción de un método para evaluar los **riesgos nuevos**, desarrollar y cambiar sistemas y para ocasiones especiales en que se hagan mayores adquisiciones e inversiones.

Las siguientes orientaciones deben tenerse en cuenta:

4.1 Política sobre Etica de los Negocios

- a) Conflictos de Interés
- b) Relación con Compradores, Proveedores y Terceros
- c) Comportamiento con Competidores
- d) Uso de la información Confidencial

- e) Relaciones comerciales internas
- f) Pago a Agentes y Comisionistas
- g) Políticas Fiscales
- h) Comportamiento frente a la Ley

4.2 Política sobre Seguridad y Controles

- a) Reglamento sobre responsabilidades de Seguridad:
 - Patrones de comportamiento
 - Procedimientos
 - Controles

4.3 Procedimientos laborales de la Empresa

- a) Evaluación de pre-empleo
- b) Clasificación y protección de la información
- c) Evaluación de nuevas inversiones
- d) Estándares de procesamiento de datos
- e) Planes de Contingencia
- f) Reportes de Incidentes
- g) Política sobre Personal

-
- h) Niveles de Seguridad
 - i) Control (Auditoría) de Cuentas

Los Contratos de trabajo deberían incluir Cláusula sobre Conflictos de Interés.

Los Bancos deben revisar de manera permanente los manuales sobre Crédito. No hacerlo podría entenderse como manifestación de negligencia de las Gerencias.

4.4 Auditoría del Seguro

- a) Selección y remuneración del Corredor
- b) Adecuación del Costo-Beneficio de la Póliza
- c) Informe de Riesgos en posesión de la Compañía de Seguros y de la Empresa
- d) Evaluación de primas, tasas y pago de indemnización
- e) Correcto cumplimiento de la Solicitud de Seguros
- f) Seguimiento a notificaciones de cambios
- g) Preservación de los sistemas de control
- h) Evaluación sobre el cumplimiento de manuales

5. Selección del Corredor de Seguros

- a) No ligados a un solo Asegurador

- b) Amplio conocimiento y experiencia del mercado específico
- c) Facilidades para ayudar en la atención de reclamos
- d) Debe vérselo como un cliente distinto, sobre el cual deben examinarse sus referencias

6. Selección del Correcto Programa

Deben examinarse las diferentes cotizaciones y considerarse todos sus elementos antes de llegar a una decisión final:

6.1 Necesidad del Seguro

En principio, el Seguro debería ser considerado como una seguridad neta para pérdidas "Catastróficas" o "Debilitantes".

Siempre que sea posible, deben aplicarse las opciones de:

- a) Asunción de Riesgos
- b) Eliminación de Riesgos
- c) Reducción de Riesgos
- d) Transferencia de Riesgos

Las empresas con altos niveles de control pueden asumir mayores deducibles. Para las de bajos controles, el Seguro no es el **remedio definitivo**.

El Seguro debe ser considerado donde la naturaleza de una operación sea tal que la efectiva de otros métodos de control de riesgos **no pueda relevarlos** y donde las consecuencias puedan afectar seriamente a la entidad en:

- a) Las utilidades
- b) Su estabilidad a largo plazo

6.2 Autoseguro

Consideración de la EAC, contra:

- a) Extensión de las coberturas
- b) Primas anuales
- c) Deducibles

6.3 Póliza y Coberturas Requeridas

No hay justificación para comprar un Seguro insuficiente. Adquirir una cobertura inapropiada o inadecuada, es imprudente y puede exponer a los directivos a responsabilidades personales; la Cobertura "fallida" puede depender de:

- a) La amplitud de los Convenios de Cobertura (monto)
- b) La claridad de los Convenios (Clausulado)

ANALISIS DE LA POLIZA

1. Coberturas

1.1 Infidelidad de empleados

- a) La forma LPD 218 es la más compleja y más restrictiva si el clausulado (no modificado) requiere prueba de deshonestidad de un empleado

irrecusablemente nominado, en tanto que en otras Pólizas se otorga protección para empleados no identificados.

- b) Las pérdidas por préstamos no están amparadas, a menos que pueda demostrarse colusión de un empleado, quien debe haber recibido beneficios económicos.

Se han dado extremos casos de intentar nulidad de la Cobertura por parte de Aseguradores, cuando sostienen que ganancias recibidas por el empleo de dinero, luego restituido por el empleado, son salarios o comisiones y no ganancias deshonestas (es necesario tener cuidado con la definición de Infidelidad).

- c) Los directores normalmente no amparados:

- Se teme que la mayoría de los fraudes ocurran por imprudencia de los niveles superiores, así que Aseguradores podrían tener la posibilidad de denegar responsabilidad de la Póliza.
- Se han dado casos increíbles en que la Cobertura para Abogados ha querido anularse al intento de considerarlos como "directores del Asegurado"

- d) Empleados temporales y auditoría externa se cubren en Hanc 83, y en la forma 24, pero están excluidos de las otras formas.

- e) Debe quedar aclarado que la Cobertura de Infidelidad es inaplicable a "Directores" y para "Crimen Electrónico".

- f) El término "intento manifiesto" encontrado todavía en algunos textos, no está definido; debería ser sinónimo de "evidente", pues la Póliza aplica a todos los casos de "responsabilidad comprobada", cuando el

empleado haya intentado o logrado causar una pérdida o daño al Asegurado.

La Prueba de persecución criminal "más allá de toda duda", no es necesaria para propósitos del seguro.

1.2 Locales

Se cubre asalto, robo, falsa pretensión, desaparición misteriosa (en términos comunes de varias formas), aunque las versiones USA restringen falsa pretensión, además de la tendencia actual de eliminarla.

Para aceptar el hecho doloso debe establecerse que el comitente está presente en el local al momento de la comisión del delito.

La cobertura puede extenderse a manipulaciones por computador y destrucción maliciosa causadas por personas distintas a empleados, siempre que el perpetrador esté físicamente en el local.

Esta cláusula no cubre ordinariamente a empleados, pero la extensión puede conseguirse mediante anexo, por una baja prima.

La cobertura restringe protección para ATM (Cajeros Automáticos), con exclusión de pérdidas causadas por vandalismo, desaparición inexplicable y mal funcionamiento de los Cajeros Automáticos.

1.3 Tránsito

En la definición del Tránsito debe tenerse cuidado con el término "al llegar a destino". que pudiera significar "lugar". La forma más completa debe decir: "Hasta entrega al destinatario designado".

1.4 Suplantación y Falsificación

Esta cláusula es menos generosa de lo que parece ser. Las definiciones y las coberturas varían ampliamente, ya que se establecen distinciones entre los dos sustantivos:

Suplantación: "Firmar con el nombre de otra persona, con el intento de engañar"; por lo tanto, no se incluye la propia firma, con o sin autoridad.

Falsificación: "Cualquier imitación que se intente para engañar y que pueda ser tomada como genuina".

Aunque toda Suplantación es Falsificación, las Pólizas operan de modo muy diferente.

En la práctica, la Falsificación (con excepción de moneda), generalmente solo aplica a:

1. Seguridades
2. Documentos de Título: B/L, Garantías de Muelle (y otros documentos que garantizan al poseedor el derecho de recibir y disponer de mercancías).
3. Hipotecas y otros
4. Certificados de Origen y Título: documentos emitidos por fabricantes sobre propiedades mobiliarias, por los cuales se transfieren los derechos.

De ordinario no se cubren documentos diferentes a los anteriores. Para que se materialice la cobertura deben tener:

- Firma falsa
- Haber sido fraudulentamente alterados
- Haber sido robados o perdidos.

Suplantación de cheques u otros instrumentos

Los cheques y otros instrumentos negociables que tengan una firma genuina, pero que sean falsos en su contenido, **no están amparados**.

En este caso se plantea la diferencia entre "falso", es decir, en los instrumentos cuyo contenido no corresponde a la verdad, y "falsificado".

La cláusula tampoco se extiende a la alteración fraudulenta y pérdida causada por una firma falsificada de una **persona no existente** (la falsificación debe corresponder a una persona cierta).

La cláusula provee alguna protección para transferencias por télex (excepto LPD 218, que es muy limitada), mientras:

- a) Sean recibidas en forma escrita, y
- b) Lleven una firma falsificada, endoso falsificado o hayan sido fraudulentamente alterados,
- c) Sean transmitidos por persona distinta al supuesto remitente

Para las empresas que tengan extensas operaciones y utilicen medios alámbricos, se recomienda examinar cuidadosamente la Cobertura, pues frecuentemente los mensajes son recibidos y almacenados en el disco del computador antes de ser impresos y distribuidos, cuando técnicamente las órdenes ya no se consideran como recibidas en una forma escrita.

(EFT "Electronic Found Transmision" no se cubre generalmente en las formas convencionales).

La forma LPO 218 restringe la Cobertura sólo para aquellos documentos en los que el empleado esté familiarizado, **de tal modo que para soportar el reclamo debe demostrarse la experiencia.**

Títulos - Valores Falsificados

Algunos entre los más grandes reclamos caen bajo esta Cláusula. Las varias formas garantizan:

- Hanc 83: Cubre Seguridades falsas, falsificadas, suplantadas, alteradas, perdidas o robadas; exige que la posesión física y real de los documentos genuinos haya sido adquirida por el Asegurado, su banco corresponsal o un representante autorizado.
- LPO 218: No tiene Cobertura similar
- 24 Standar: Aplica a suplantación, pérdida y alteración; sólo cubre falsificación de cualquier original de un Título -Valor, Hipoteca, Certificado de Origen o de Propiedad.

Moneda Falsificada

La Cobertura ordinariamente se limita a la moneda de circulación en el país; en las versiones más modernas se ampara la moneda de todos los países.

Pérdidas Comerciales

- En Hanc 83 El término "Comercial" usado en esta Póliza, debe ser entendido como la comercialización o el manejo de seguridades, bienes, futuros, opciones, fondos de gobierno, cambio extranjero y similares.

- Si la pérdida es causada (promovida por un empleado), se requiere probar la ganancia personal (prebenda o soborno). LPO 218 es la forma más exigente.
- En 24 Stdr No se ampara Pérdida Comercial ni aún cuando un empleado actúe deshonestamente.

Préstamos

Las pérdidas por Préstamos otorgados cuando un empleado actúe deshonestamente, están amparadas en todas las formas convencionales.

Daños a Oficinas/Locales

Para garantizar el Amparo debe establecerse que la finalidad sea el cometimiento de un acto doloso. Si esta Cobertura es concurrente con Pólizas de Daños materiales podría conseguirse eventual rebaja de primas.

Endoso de Cajeros Automáticos

Ampara pérdidas de Cajeros Automáticos y máquinas similares ubicadas en locales del Asegurado.

Las pérdidas originadas por vandalismo, uso de Tarjetas de crédito o Débito, falla de las máquinas, están generalmente excluidas.

Extorsión

Provee protección para pago de rescate de un empleado o funcionario del banco que sea secuestrado, con el objeto de obtener recompensa.

EFTS (Transferencia Electrónica de Fondos)

El anexo enmienda el Amparo de Falsificación. Cubre las instrucciones fraudulentas para transferir fondos, por o en nombre del Asegurado, mientras:

- a) Las instrucciones ingresen entre los terminales de la red del Sistema cubierto.
- b) Cuando ingrese por una persona que aparente representar a una institución autorizada para utilizar el Sistema cubierto.

(No se amparan instrucciones telefónicas)

Endoso de Instrucciones Orales

Se extiende el Amparo para instrucciones orales o telefónicas.

Cajas de Seguridad para Depósitos

Provee Cobertura para este medio, que actualmente ha sido retirado de las Pólizas convencionales.

Tarjetas de Crédito y Débito

Se amparan pérdidas por el mal uso de estas tarjetas.

Exclusiones

Deben examinarse todas, a fin de identificarlas con los riesgos.

Coberturas Existentes para Crimen Electrónico

1. LECCP, de Lloyd's de Londres

2. Shand Morahan Unauthorized Acces Policy (USA)
 3. Anexo a Forma 24 Std
 4. Fianza Comercial de AIU
1. **LECCP**

(Se emitió como contraparte de Hanc 83) excluye todos los amparos concedidos bajo Blanket Bond y todo los actos de empleados; la versión de 1.981 fue completamente inoperante , pero luego se mejoró. Se garantizaban las pérdidas en exceso de la primas brutas

La Póliza tiene 7 convenios, que pueden ser suscritos a discreción:

CONVENIOS, LECCP		
Número	Actuación Cubierta	Objeto Asegurado
1	Actos Fraudulentos	Datos Electrónico
2	Preparación	Fraudulenta. Programas
3	Dstrucción Maliciosa	Datos y medios electr.
4	Fraude	Transfer. por télex,simil.
5	Fraude	Operaciones en Computador
6	Fraude	Entrada de transf. por télex
7	Fraude	Instrucciones orales

La Póliza en general comienza a responder por actos directamente causados contra el sistema de computación del Asegurado, pues está diseñada para cubrir solamente fraudes por medios técnicos dependientes del computador, así que, la entrada fraudulenta a través de un terminal, está excluida.

2. Shand Morahan

La Póliza se compromete por el acceso no autorizado, en una amplia definición de pérdida, incluida Responsabilidad Legal y Costos Indirectos. Explícitamente ampara transferencias fraudulentas por medios alámbricos, destrucción maliciosa, pérdida de datos confidenciales y otros actos que concluyan en pérdida.

(La Póliza salió del mercado en 1.985, debido al balance desfavorable entre siniestros y primas).

3. Anexo a Formas 24 y 22 Std

Cubre transferencias electrónicas fraudulentas (entrada y salida), daño malicioso (sujeto a Cláusulas de Pérdida y Ganancia) y cambios al programa.

El anexo es más generoso que LECCP, pues cubre falsos códigos de barra y otros medios óptico-mecánicos.

4. Anexo a Fianza AIU

Incluye acceso fraudulento al Sistema, inserción de datos fraudulentos, alteración de datos y programas, sin necesidad de probar ganancia personal, pero excluye daño malicioso, pérdida de datos confidenciales y costos indirectos.

LA COBERTURA Y LOS OBJETIVOS

1. Información Confidencial

En todas las pólizas, excepto Morahan, la pérdida de información confidencial está específicamente excluida, LECCP excluye todas las pérdidas resultantes directa o indirectamente del acceso a cualquier información confidencial,

incluyendo, pero sin limitar, a secretos comerciales, programas de computación o informaciones de usuarios.

En teoría, si una persona accesa información confidencial (como por ejemplo, una contraseña) y después usa esta información para defraudar, por un acto que pudiera caer bajo el amparo de Infidelidad, el Asegurador niega responsabilidad.

2. Responsabilidad Legal y Pérdidas Indirectas

La Póliza Shand Murahan cubre la responsabilidad legal que recaiga contra el Asegurado como resultado de acceso no autorizado al Sistema LECCP provee similar protección bajo la Convención 5, cuando el Asegurado actúe como empresa de Servicios, y bajo la Convención 6, de transferencias dolosas por sistema alámbrico. Las otras Pólizas no proveen protección equivalente.

Shand Morahan incluye los costos adicionales de la conducción del negocio, pérdida de tiempo del Computador, pérdida de dinero o seguridades y otras pérdidas que el Asegurado pueda sufrir durante los 12 meses siguientes a la fecha de descubrimiento del acceso no autorizado. (La cantidad que se pueda recobrar, es materia de debate).

3. Seguridades

LECCP provee reembolso por la pérdida o robo de seguridades, pero sólo cuando sean cometidos en la forma de datos electrónicos, en tanto Shand Morahan cubre la pérdida resultante del acceso no autorizado, de cualquier modo que sea.

4. Medios de Procesamiento de Datos

Se ampara el valor en blanco de los medios, más el trabajo de copiado.

5. Salas de Cómputo

No están amparadas en ninguna Póliza, excepto LECCP (a menos que tales facilidades se incluyan como parte del Sistema del Asegurado), y limita la protección a la modificación fraudulenta de ingresos o a la destrucción maliciosa de medios.

LA COBERTURA DEPENDE DE LA MOTIVACION (INTENCION)

Las varias Pólizas encaran de manera diferente la cuestión de motivación para el cometimiento de actos fraudulentos o deshonestos:

1. Fraude

- a) LECCP requiere prueba de intención de causar al Asegurado una pérdida, o de obtener una ganancia personal por parte del perpetrador u otro.
- b) Shand Morahan no requiere prueba de la intención, sino la realización de ingreso no autorizado, **lo cual es difícil de probar.**
- c) AIU y Forma 24, son más amplios:
 - AIU ampara acceso fraudulento e inserción fraudulenta de datos
 - Forma 24 requiere prueba de intención manifiesta.

2. Malicia

- LECCP no cubre los actos motivados por malicia, excepto bajo la Convención 3A, cuando los datos electrónicos son almacenados (no transmitidos) dentro del Sistema del Asegurado. Bajo la Convención 3B, la intención (motivación) no es necesario de ser probada en casos

de pérdidas por desaparición misteriosa y robo de medios de computación.

- Shand ampara pérdidas si se derivan de ingreso no autorizado. Los daños por incendio malicioso no están amparados por ninguna Póliza.

3. Extorsión

Generalmente excluida, pero Shand, Morahan y LECCP pueden extender la Cobertura, siempre que no haya colusión con ningún empleado.

4. Anexos

La gran experiencia ha hecho que los Reaseguradores tengan preparados Anexos para ampliar o limitar la Cobertura.

5. Exclusiones Importantes

Las Pólizas son muy diferentes en su lenguaje y construcción, por lo cual es difícil comparar las Exclusiones. Cada una habla de la posibilidad de negar el reclamo. No obstante, las siguientes son las más peligrosas, debido a que son "abiertas" y de muy amplia interpretación:

- a) Extorsión contra empleados
- b) Colusión
- c) Acceso a información Confidencial
- d) Daño Mecánico
- e) Errores en Programación
- f) Compra de programas

CONCLUSIONES

La complejidad de éstas Pólizas hace muy difícil decidir cuál es más apropiada; cada una usualmente limita sus beneficios, de tal modo que ninguna puede ser vista como una panacea contra el fraude por computador.

SEGURO DE RESPONSABILIDAD DE DIRECTORES Y FUNCIONARIOS

- El Tercero/usuario Reclama contra Funcionario (Demanda Legal)
 - La Compañía de Seguros Paga
 - El Banco o la Entidad Financiera se ve libre de la acción del tercero/usuario
1. La indemnización de responsabilidades para Directores y Funcionarios, presentes o pasados (inclusive fallecidos), se denomina "blanket".

No cubre actos de deshonestidad ni ganancia personal, sino fallas y errores en casos que de ordinario comprendan Pérdidas excesivas y Negligencia

Debe señalarse que la Cobertura no se refiere a responsabilidades de la empresa, sino de las personas.

2. Reembolso Corporativo: paga a la empresa cuando esta reembolsa a Directores y Funcionarios por sus responsabilidades. La Cobertura correspondiente se adquiere por Convención Especial.

Para la aceptación de responsabilidad debe entenderse:

- a) Reclamos legales instaurados en la vigencia de la Póliza

b) Notificación de intento de acción (Reclamo), a la Junta de Directores.

Los Directores o Funcionarios, deben estar desarrollando sus "tareas propias" al momento de alegada falla.

Se recomienda para este amparo, eliminar la Exclusión de Asegurado contra Asegurado.

Nota: En las Pólizas Bancarias, se excluye obligación de indemnizar en caso de que cualquier pérdida resulte de insolvencia del Asegurado.

LIMITES ASEGURABLES

1. **Límites Asegurables en Infidelidad:** Las siguientes bases permiten analizar la suma asegurable:

- a) Total de los Activos
- b) Movimiento
- c) Utilidades
- d) Monto de los depósitos (Bancos)
- e) Préstamo límite (Bancos)

Debe considerarse si la suma se fija por:

- 1. límite individual de pérdida
- 2. límite agregado

Puede suscribirse:

1. Cobertura base para Infidelidad
2. Cobertura de Exceso para Infidelidad
2. Crimen por Computador

El problema no es tanto determinar la Suma Asegurable, sino la escogencia de la Póliza de mayor conveniencia.

3. D & O (Directivos y Funcionarios)

El límite asegurable puede igualarse al de Infidelidad, aunque la actual tendencia en Inglaterra y Estados Unidos, es concederle mayor cantidad.

Límite Asegurable				
	Total Retiros	Riesgo Bajo	Riesgo Alto	Deducible
hasta US\$	25.000.000	2%	8%	4%
	100.000.000	2%	4%	2%
	500.000.000 0.	8%	1.6%	1%
	1.000.000.000 0.	8%	1.5%	0.5%
	5.000.000.000 0.	3%	0.8%	0.2%
s/Movimiento		10%	15%	
s/Utilidades		0.5% Año	1.0 Año	
S/Monto Depósito		2%	4%	
s/Préstamo Límite		50%	80%	

4. Cobertura Individual o Agregada

Individual: Reinstalación automática

Agregada: Agotamiento

5. Descubrimiento Vs Ocurrencia

Descubrimiento:

- a) Ampara las pérdidas descubiertas durante la vigencia de la Póliza
- b) Se extiende a amparar las pérdidas dentro período de Retroactividad

Ocurrencia :

Cubre la pérdidas ocurridas y reportadas a Compañía, dentro de la vigencia de la Póliza.

CARACTERISTICAS DE CUBRIMIENTO				
Póliza	Descubrim.	Ocurrencia	Retroact.	Extensión desc.(meses)
LPO 218	--	sí	sí	- no -
Hanc 83	sí	--	no	12
24 Stdr	sí	--	no	12
*24 Revisd.	sí	--	no	- no -
Guarantee Sc	--	sí	--	18
Stdr Forma A	--	sí	--	12
AIU	--	sí	--	24
LECCP	sí	--	--	12
Shand M.	--	sí	(a convenir)	12
Anexo 24	sí	--	--	- o -
Anexo AIU	--	sí	--	24

Límite Agregado:

Surety Association of America, señaló que: "es imperativo que cada Asegurador tenga una firme idea de su posible máxima responsabilidad por un período de tiempo fijo"; cuando concede Límite agregado.

Observación:

Debe tenerse especial cuidado en el cambio de Aseguradores o de Formas, para no dejar posibles pérdidas desprotegidas.

Si no resulta posible negociar la Póliza de Descubrimiento, la de Ocurrencia puede beneficiarse:

- a) Con período de Retroactividad
- b) Con período de descubrimiento después de vigencia

6. Escogencia del Mercado: Pólizas Centralizadas y Locales

Características	
Centralizadas	Locales: Afiliadas
1. Deben ser consistentes con los niveles de riesgo de todos los afiliados. 2. Si el Asegurado tiene un Gerente de Riesgo Corporativo, que puede vigilar y mantener la Cobertura 3. Estilo de Gerencia Centralizado 4. Estructura de Holding	1. Atienden particularmente a los altos riesgos específicos. En este caso la negociación de prima individual es preferible 2. No hay generalmente funciones de Administrador de Riesgo 3. Control descentralizado 4. Estructura descentralizada

Relaciones con Asegurador	
A. Procesamiento integrado de datos en sistemas abiertos	A. Procesamiento local: Red Limitada
B. Operaciones complejas, que requieren coordinar Infidelidad, ECC, D & O	B. Operaciones simples en todas las empresas afiliadas
C. Requerimientos estatutarios para mantener la Cobertura extendida a todas las operaciones	C. Requerimientos limitados
D. Menores tasas de Cobertura	D. Mayores tasas de Cobertura
E. Cláusulas comprensivas de Cobertura. (Cláusulas de restricción en mercados locales)	E. Cobertura flexible, comprensiva o restringida, en mercados locales.
F. Límites Asegurables y deducibles	F. Límites Asegurables y deducibles

7. Escogencia del Asegurador

- a) Debe estudiarse el Índice de solvencia
- b) Hay que aceptar que la mejor Póliza no es necesariamente la más económica en primas
- c) Para Compañías asociadas, aunque haya algunas ventajas en suscribir la Póliza en forma global, por cuanto en caso de reclamo puedan

originarse problemas, es preciso que el Asegurador consulte con el Reasegurador sobre ciertas decisiones.

La distribución del Seguro con otros Aseguradores locales puede ser beneficiosa, pues da al primero (Asociado) un derecho de consulta local.

8. Primas

Los Reaseguradores no revelan sus métodos de cálculo (de 0.5% tasas han subido hasta el 12%; para Riesgos mayores, se estudia la pérdida anual probable: Frecuencia x Severidad).

9. Vigencia de la Póliza

- a) Para efectos de la responsabilidad en la Forma "Descubrimiento", la fecha de retroactividad inicia válidamente la vigencia de la Póliza.
- b) Sobre la Vigencia actual se calcula la prima básica
- c) Continuidad de períodos: la Cobertura, aunque se extienda desde la primera vigencia, da al Asegurado el derecho de reclamar según los límites al momento de la Ocurrencia (los límites no son acumulativos)
- d) Las Formas Sdtr "A", AIU y Guarantee Soc., conceden, sin pago de prima, un período para reportar las pérdidas después de la vigencia de la Póliza, siempre que estas hubieren tenido lugar dentro del tiempo de Cobertura (Vigencia)
- e) Derechos después de cancelación: LECCP, Hanc 83, Sdtr 24 (no Sdtr revisada), proveen extensión de tiempo para Descubrimiento, bajo Prima Adicional.

10. Nombre del Asegurado

Los beneficios están limitados al Asegurado nominado, pero con permiso del Asegurador pueden extenderse a otros entes que tengan intereses con aquel.

Los nuevos locales, nuevos empleados, ampliación de las operaciones y sistemas de computación, quedan automáticamente amparados en todas las Formas.

11. Beneficios de la Póliza

- a) Los beneficios de las Pólizas son exclusivamente en favor del Asegurado.
- b) En USA hay abierta oposición a que alguna Autoridad Federal se envuelva en los negocios del Asegurado.
- c) Todas las Pólizas operan en Exceso de cualesquiera otras que sean concurrentes.

12. Notificación de Cambios

- a) Por regla general el Asegurado prefiere someterse sólo a un limitado número de ocasiones para notificar al Asegurador los cambios de su negocio
- b) Los Actos deshonestos de empleados antes del inicio de la vigencia de la Póliza, deben ser comunicados al Asegurador con toda precisión.
- c) El crecimiento orgánico se encuentra automáticamente amparado: nuevas oficinas/empleados
- d) Las fusiones, adquisiciones o embargos deben ser notificados al Asegurador en término de 30 días desde su ocurrencia

- e) **Guaranteee Soc., exige aviso de cambio en la naturaleza del negocio:**
banco- Compañía Financiera/Compañía de Préstamos.

13. Notificación de Pérdidas

Debe darse al Asegurador en forma inmediata a su descubrimiento.

14. Valuación

- a) En Pérdida de datos: valor de reconstrucción de documentos
- b) En Pérdida de Seguridades: valuación a su vencimiento
- c) En Moneda Extranjera: de acuerdo a Cotizaciones Bursátiles
- d) En Productos aunque ninguna Póliza establece método como el caso de Almacenes Generales de Depósito debe determinarse su Valor de Reposición para la fecha del accidente.

15. Subrogación

16. Salvamento y Recuperación

- a) Reembolsos en gastos/costos de recuperación
- b) Exceso de la pérdida sobre límites amparados (neto de deducible)
- c) Reembolso al Asegurador
- d) Para estitución del Deducible.

17. Cómputo de la Pérdida

- a) Se excluyen ingresos potenciales para el Asegurado (intereses, dividendos)
- b) Se excluyen pérdidas indirectas o consecuenciales.

18. Costas, Servicios de Defensa, Arbitramento

- a) En USA, cada parte cubre gastos de defensa
- b) En UK y en la mayor parte de los países, reembolsa el perdedor
- c) Arbitramento: Cada parte asume los gastos y costos.

El Arbitramento puede invocarse por Diferencias Irreconciliables en:

- Interpretación de la Póliza
- Valuación de las Pérdidas cubiertas.