TECNOLÓGICO UNIVERSITARIO DE MÉXICO

ESCUELA DE ADMINISTRACIÓN

INCORPORADA A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
CLAVE 3079-02

“LA GESTIÓN DE RIESGO EN EL ÁREA DE CONTROL INTERNO DE UNA INSTITUCIÓN BANCARIA”

TESIS

QUE PARA OBTENER EL TÍTULO DE:

LICENCIADA EN ADMINISTRACIÓN

PRESENTA:

RUTH GARCÍA SÁNCHEZ

ASESOR DE TESIS: LIC. ARNULFO VEGA VÁZQUEZ

CIUDAD DE MÉXICO **2018**

“LA GESTIÓN DE RIESGO EN EL ÁREA DE CONTROL INTERNO DE UNA INSTITUCIÓN BANCARIA”

Introducción.

Durante nuestra experiencia universitaria los temas de control interno suelen ser abordados muy poco, la información teórica suele ser escasa sin tener la oportunidad de poder explorar el tema a profundidad, el conocimiento de ello se va adquiriendo en la práctica laboral, una vez que nos enfrentamos a un caso real en el cual podemos percibir los riesgos que implican el ejecutar procesos sin un sistema de control interno que resguarde lo que estamos realizando.

La presente tesis tiene como objetivo presentar la importancia de aplicar el control interno en una institución financiera de una manera clara y objetiva, por medio de casos prácticos que nos facilitan comprender la teoría de una manera más amigable; cabe mencionar que los controles financieros son muy robustos, por lo cual también pueden ser aplicados a cualquier tipo de institución, adecuándolos a sus necesidades, debilidades y fortalezas encontradas.

A lo largo del presente trabajo se podrá observar que el sistema de control interno es un conjunto de planes y metodologías cuya finalidad es proteger los recursos de la institución, ya que la inexistencia de estas acciones puede ocasionar perdidas de dinero, confidencialidad e integridad de la información, generando no solo un impacto económico sino también reputacional y/o regulatorio, que podrían poner en duda la seguridad utilizada para proteger y resguardar la información y/o activos que los clientes han proporcionado.

En la actualidad existe una variedad de formas de cómo y quién puede atacar la institución, es decir, el riesgo puede presentarse del interior de la institución debido a empleados coludidos con personas externas; adicionalmente la presencia de otros factores internos como errores en los sistemas, fallas en los procesos, la inexistencia de un área de control, falta de información y comunicación, entre otras; o puede llegar por una fuente externa a la institución, como grupos organizados para efectuar lavado de dinero, fraude, robo de información y/o identidad, etc., por ello es importante la creación del control interno y sus diversas metodologías, para efectuar acciones y medidas como:

1. Segregación de funciones.
2. Definición de procesos, así como también la identificación de las personas involucradas y las facultades necesarias para la correcta ejecución de sus actividades.
3. Políticas que contengan la parametrización de controles aplicables a cada uno los procesos, por ejemplo, política anti-fraude, prevención de lavado de dinero, código de conducta, etc.
4. Constante capacitación y comunicación a los empleados.
5. Crear modelo de seguridad de la información, para la protección, categorización y manejo correcto de los datos involucrados en la institución.
6. Supervisiones continuas de la correcta aplicación de los controles por parte de los empleados.

7. La correcta identificación de nuestros clientes, a través de la metodología conoce a tu cliente “KYC”.

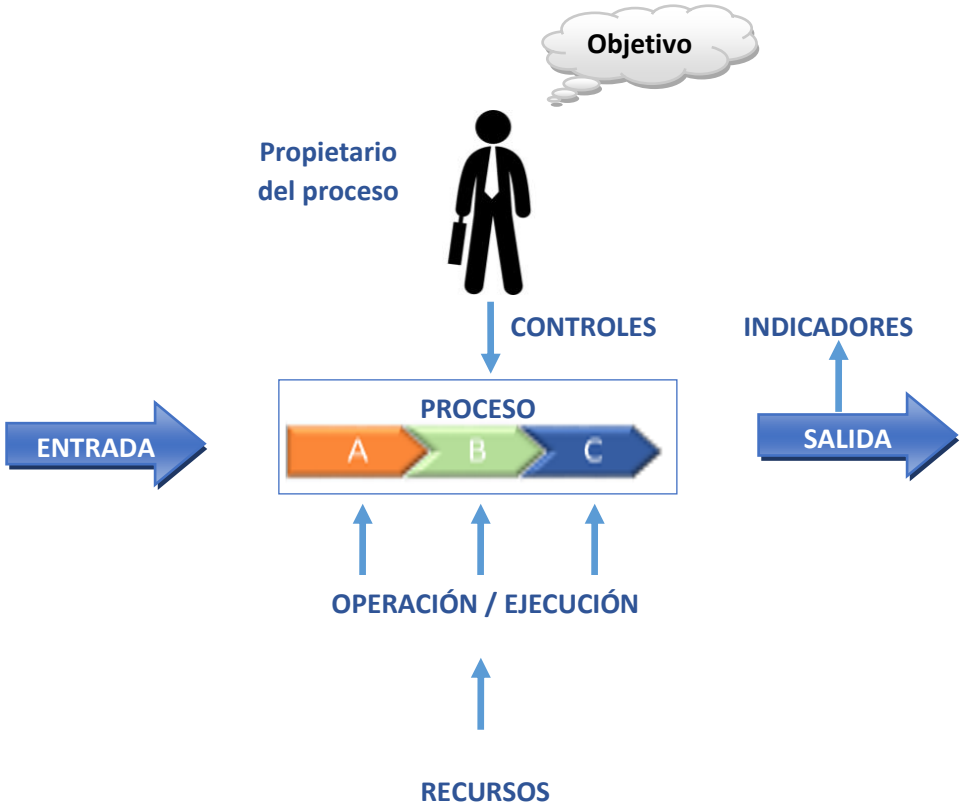
La correcta evaluación de riesgos y la aplicación del control interno nos podrá garantizar el contar con una institución protegida y empleados capacitados para mitigar las amenazas existentes.

Capítulo 1 Procesos, Riesgos y Controles.

1.1 Proceso, definición y sus generalidades.

De acuerdo a ISO 9001 Proceso es un conjunto de actividades mutuamente relacionados o que interactúan, las cuales transforman elementos de entrada a resultados.
Todo proceso es un conjunto de tareas elementales necesarias para la obtención de un resultado. Cada proceso posee unos límites claros y conocidos (primer paso y último paso) comenzando con una necesidad concreta y finalizando una vez que la necesidad ha sido satisfecha. [1]
Proceso: serie de acciones sistemáticas dirigidas al logro de un objetivo. [2]
Como proceso podemos entender que es un conglomerado de actividades interrelacionadas, mediante las cuales agregamos un valor a las entradas (pudiendo ser materiales o inmateriales) con el objetivo de poder suministrar, productos, servicios e información a nuestros clientes externos o internos.

ELEMENTOS DE UN PROCESO.



[1] Pérez Fernández José Antonio / Gestión por procesos como utilizar ISO 9001 2000 / Editorial ESIC.

[2] Juran J. Juran / Planificación de la calidad / Ediciones Díaz de Santos.

A continuación, se explica el mapa anterior:

Propietario de proceso: se considera al empleado como dueño de su proceso, lo cual nos permitirá que este sentimiento de propiedad contribuya a su alta motivación y realización adecuada de sus actividades; adicionalmente es el empleado quien se vuelve responsable de sus procesos, por ello es importante que el empleado conozca la finalidad e importancia de sus funciones que pueden impactar o beneficiar a toda la organización.

Entrada: son los requerimientos de una necesidad de un cliente interno o externo, la existencia de ello es lo que justifica la ejecución del proceso.

Recursos: son los medios y las herramientas mediante los cuales se lleva a cabo el proceso.

Controles: es el establecimiento y aplicación de indicadores, objetivos, directrices y políticas en la ejecución de proceso, siendo fundamentales para evaluar la marcha en el proceso y corregir las deficiencias oportunamente, lo cual nos permitirá cumplir al 100% con el objetivo del proceso.

Indicadores: es aquel soporte de información, normalmente representado por medio de métricas que nos ayudarán a analizar la eficacia y la eficiencia del proceso mediante la presentación de aquellas variables que nos permitirán observar defectos o errores en el proceso evaluándolo para poder realizar la toma de decisiones y obtener una mejora continua.

Salida: es aquel producto o servicio final que será entregado a nuestro cliente interno o externo.

1.2 Definición de riesgo.

Riesgo: es la probabilidad y su posible impacto, de que un evento adverso obstaculice o impida el logro de los objetivos y metas institucionales, o que incida negativamente en el funcionamiento y resultados de la entidad.[3]

Riesgo: se produce cuando hay probabilidad que algo negativo suceda o que algo positivo no suceda, la ventaja de una empresa es que conozca claramente los riesgos oportunamente y tenga la capacidad para afrontarlos.[4]

Riesgo, es la probabilidad que un peligro (causa inminente de pérdida) existente en una actividad determinada durante un período definido, ocasione un incidente con consecuencias factibles de ser estimadas.

[3] Santillana González Juan Ramón / Sistema de Control Interno / Editorial Pearson Tercera Edición.

[4] Estupiñán Gaitán Rodrigo / Administración de Riesgos E.R.M y la Auditoria Interna / Editorial ECOE Ediciones.

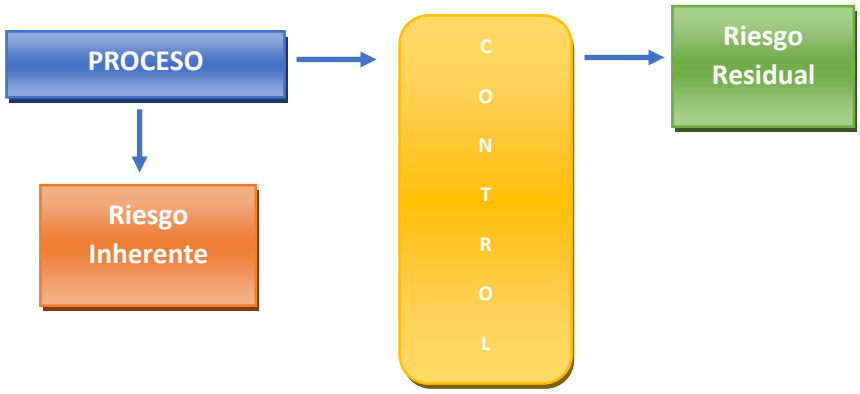
Consideraremos riesgo a todas aquellas acciones que puedan generar resultados adversos para el cumplimiento de los objetivos, perjudicando a una organización empresarial.

El origen del riesgo puede ser derivado por amenaza externa, competencia desleal o debilidad interna

La correcta y oportuna identificación de los riesgos pueden marcar la diferencia entre el éxito y fracaso de una empresa.

Es importante tener presente que en muchas ocasiones los integrantes de un equipo conocen los riesgos, pero no los comunican en la forma adecuada. Por lo general, en la cadena de mando es más fácil informar de los riesgos hacia abajo, pero es difícil hacerlo en sentido contrario. En todos los niveles, las personas pretenden conocer los riesgos de los niveles inferiores, pero muchas veces no los comunican abiertamente a quienes están a un nivel más alto.

1.2.1 Tipos de riesgos y como mitigarlos.



Al momento que nace un proceso, de la mano nacé el riesgo inherente.

Riesgo Inherente: representa el riesgo de que ocurran errores importantes en un tipo específico de proceso o actividad, o en un rubro específico de los estados financieros (cuenta, saldo o grupo de transacciones), en función de la naturaleza, características o particularidades del negocio, sin considerar el efecto de los procedimientos del control interno que pudieran existir.[5]

[5] Santillana González Juan Ramón / Sistema de Control Interno / Editorial Pearson Tercera Edición.

Riesgo Inherente son aquellos errores o irregularidades significativas resultantes durante la aplicación del proceso antes de considerar la efectividad de los sistemas de control, también podemos identificarlo como aquel que es propio del trabajo o proceso, que no puede ser eliminado del sistema; es decir, en todo trabajo o proceso se encontrarán riesgos para las personas o para la ejecución de la actividad en sí misma.

Por ello es importante conocer su causa, que es la que va a determinar la existencia de este y si puede afectar a la empresa o no, es importante identificar aquellos eventos y riesgos potenciales que pueden llegar a afectar la implementación de estrategias o el logro de los objetivos con impactos positivos, negativos o ambos, para ello es necesario el “Control” ya que ayudará a mitigar o reducir los riesgos.

Cabe mencionar que un riesgo inherente jamás va a desaparecer, ya que no existe un control perfecto que lo elimine, lo cual nos da como resultado el riesgo residual, es aquel remanente que permanece después de haber implementado los controles.

Riesgo residual: es aquel riesgo que subsiste después de haber implementado controles, puede verse como aquello que separa a la compañía de la seguridad absoluta.

El riesgo residual o también conocido como riesgo prevaleciente es aquel que continua después de haber aplicado algún sistema de control, nuestro riesgo residual puede ser tan grande o tan pequeño de acuerdo a los tipos de controles que se hayan implementado, es por ello que también debe hacerse un análisis al igual que con el riesgo inherente:

1. Identificar el riesgo.
2. Tratar de mitigarlo hasta un nivel aceptable.
3. La Dirección deberá decidir hasta que nivel puede ser aceptable el riesgo, tomando decisiones y acciones conducentes para mitigarlo.
4. Evaluar si el costo de reducir el riesgo es mayor al mismo costo del riesgo.

Tipos de riesgos que se manejan en una institución Bancaria.

1. Riesgo operativo: es la posibilidad de pérdidas originadas por fallas o insuficiencias en procesos, sistemas, personas o eventos externos imprevistos.

El comité de Basilea lo define como: aquel que proviene de fallas de información en los sistemas o en los controles internos que pueden provocar una pérdida inesperada. Este riesgo se asocia con errores humanos, fallas en los procesos e inadecuados sistemas y controles.

De acuerdo con José Antonio Núñez y José Juan Chávez, en su artículo “Riesgo operativo: esquema de gestión y modelado del riesgo”, del riesgo operativo se pueden destacar las siguientes características:

a) Es antiguo y está presente en cualquier clase de negocio.

b) Es inherente a toda actividad en que intervengan personas, procesos y plataformas tecnológicas.

c) Es complejo, como consecuencia de la gran diversidad de causas que lo originan.

d) Las grandes pérdidas que ha ocasionado en varias empresas, muestran el desconocimiento que de él se tiene y la falta de herramientas para gestionarlo.

2. Riesgo de fraude: es la acción intencional de una o más personas, que buscan obtener ventaja sobre la organización, por medio de conducta deshonesta o engañosa, algunas de sus causas son las siguientes:

a) Poco cuidado u omisión de los controles por parte del dueño del proceso.

b) Omisiones de cantidades o engaños en elaboración de estados financieros.

c) Desviación de dinero o fondos a cuentas externas de la institución bancaria.

d) Incentivos por parte de fuentes externas para apropiarse indebidamente de activos que involucren el robo de los recursos de la empresa.

3. Riesgo de lavado de dinero: según la CNVB (Comisión Nacional Bancaria y de Valores) lo define como el proceso a través del cual es encubierto el origen de los fondos generados mediante el ejercicio de algunas actividades ilegales o criminales (tráfico de drogas o estupefacientes, contrabando de armas, corrupción, fraude, prostitución, extorsión, piratería y últimamente terrorismo).

Algunas causas son:

a) Transacciones inusuales de un cliente.

b) Antecedentes comerciales del cliente difusos o inexistentes.

c) Comportamiento inusual del cliente, nerviosismo o negación al brindar información.

4. Riesgo reputacional: es aquel que se deriva de la percepción u opinión negativa del cliente respecto al servicio proporcionado por el banco, generando un impacto negativo en la mala imagen o posicionamiento negativo en la mente de los clientes existentes o futuros, disminuyendo la credibilidad que se tenga hacia la institución.

5. Riesgo regulatorio: es aquel que surge por el incumplimiento de políticas, leyes y reglas establecidas por una institución regulatoria encargada de establecer los lineamientos a seguir.

6. Riesgo tecnológico: es la pérdida de información potencial por daños, interrupción, alteración o fallas derivadas de software, hardware o cualquier otro canal donde se transmita o proporcione información de los servicios proporcionados por la institución o información perteneciente al cliente.

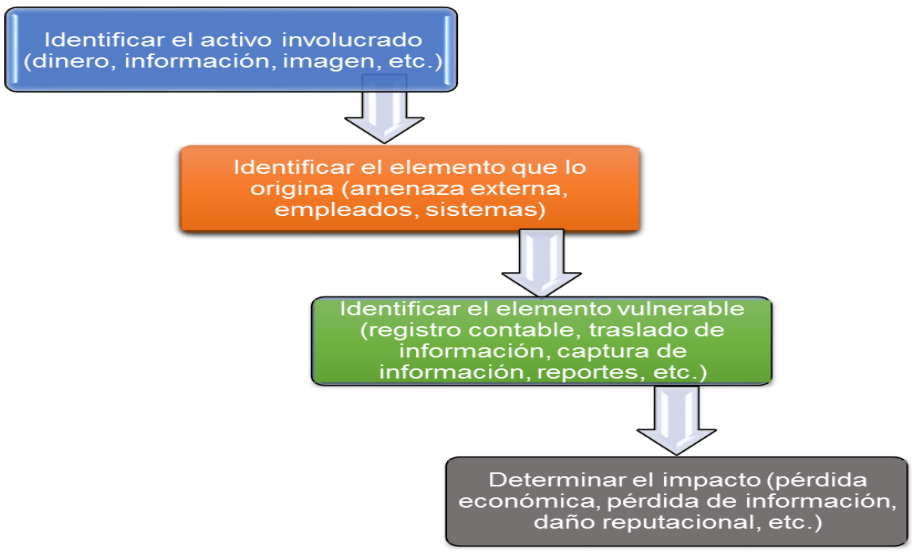
7. Riesgo estratégico: es aquella pérdida como resultado de fallas o deficiencias en la toma de decisiones, en la implementación de los procedimientos y acciones para llevar a cabo el modelo de negocio o estrategias que estén por ser implementadas para la mejora de la institución en general o de un proceso, por ejemplo, la creación de un nuevo producto, la fusión con alguna empresa, etc.

Para poder mitigar el riesgo, es importante implementar el “Control”, ya que son las acciones y medidas que permitirán conocer y dimensionar todos los elementos relacionados con los riesgos para poder hacer frente a ellos permitiendo reducir los errores en el proceso, por lo cual es imprescindible que los dueños de los procesos creen conciencia de los riesgos que se pueden presentar y los efectos derivados de ellos.

Una actividad del control es la administración del riesgo, está compuesta por el conjunto de procedimientos para identificar, analizar, evaluar y controlar los efectos adversos de los riesgos a los que está expuesta la institución. Su principal propósito es evitarlos o reducirlos.

La evaluación del riesgo implica un proceso dinámico e interactivo para identificar y evaluar los riesgos de cara a la consecución de los objetivos. Una condición previa a la evaluación de los riesgos es el establecimiento de objetivos asociados a los diferentes niveles de la institución, por lo que requiere que la Dirección considere el impacto que puedan tener posibles cambios en el entorno externo y dentro de su propio modelo de negocio, que puedan provocar que el control interno no resulte efectivo.

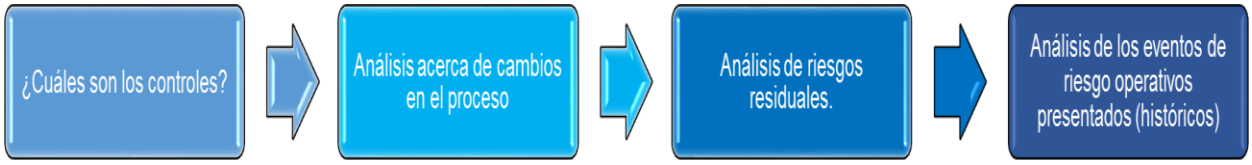
ELEMENTOS PARA DESCRIBIR O IDENTIFICAR EL RIESGO.



¿CÓMO ANALIZAR EL RIESGO?

Para poder identificar el riesgo al cual nos enfrentamos nos podemos apoyar en contestar las siguientes preguntas:

ANÁLISIS DEL ELEMENTO VULNERABLE.



ANÁLISIS DEL IMPACTO.

ANÁLISIS DEL RIESGO DE REVISIÓN.

Monitoreo para analizar qué tan expuesto estoy al riesgo y asegurar los controles efectivos hacia cada proceso.

El análisis de riesgos nos permitirá observar las amenazas a las cuales está expuesta la institución y tomar las medidas correctas para su protección.

El proceso de análisis de riesgos debe de estar documentado para poder tener el soporte que nos ayudará a justificar las acciones que se van a desarrollar.

1.3 Establecimiento de control interno y su monitoreo.

1.3.1 Definición y objetivo del control interno.

Control Interno: es un proceso, efectuado por el consejo de Administración, la Dirección General y el resto del personal de la institución, diseñado para proporcionar un grado de certeza razonable en cuanto a la consecución de los objetivos.[6]

El control interno es el conjunto de planes, medidas, acciones, métodos y procedimientos diseñados y efectuados para limitar los riesgos que afecten las actividades de la institución bancaria a través de la investigación y análisis de los riegos. Los controles siempre están dirigidos a acciones o reacciones buscando que el proceso cumpla con su objetivo, mitigando aquellos riegos que puedan estar implícitos en ellos.

Un buen control interno proporciona la base para mantener en dirección hacia la consecución de los objetivos y minimizar posibles riesgos y sorpresas adversas en el camino.

Podríamos considerar al control interno como:

1. El corazón de la Institución.
2. La cultura, normas sociales y ambientales que gobiernan a la institución.
3. Las políticas, actividades y procedimientos por los cuales se mueve la institución.

[6] Committee Of Sponsoring Organizations of the Treadway Commission (COSO).

Dentro de sus principales objetivos podremos encontrar:

a) Definir y aplicar medidas para prevenir riesgos, detectar y corregir las desviaciones que se presenten al momento de efectuar un proceso.

b) Proteger los recursos de la institución bancaria evitando perdidas por fraudes, negligencias, etc.

c) Asegurar la exactitud y veracidad de la información.

d) Estimular el seguimiento de tareas ordenadas.

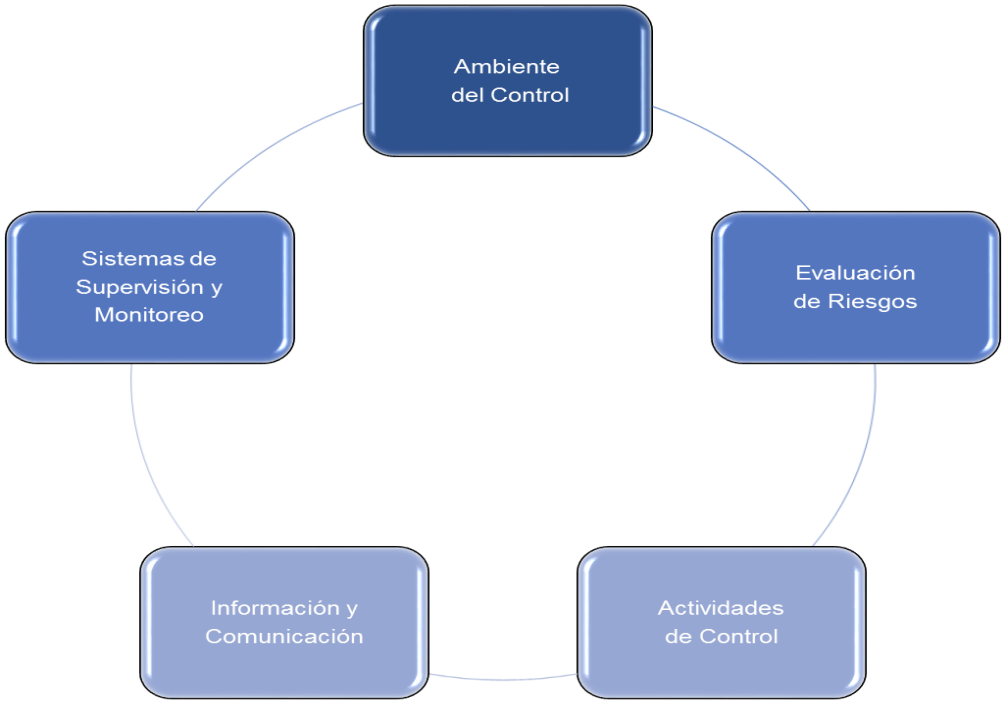
e) Cumplimiento con los requerimientos regulatorios aplicables.

f) Establecer metodologías de análisis y evaluación de riesgos.

g) Identificar fuentes de información adecuadas para medir la magnitud de los riesgos.

Su principal característica es que debe dejar evidencia de su existencia, de no ser así se da por entendido que el control no sirve o simplemente no existe.

COMPONENTES DEL CONTROL INTERNO.



1. Ambiente del control: este componente ayuda a proporcionar disciplina y estructura, ya que es el conjunto de normas, procesos y estructuras que constituyen la base sobre la cual se desarrolla el control interno; incluye la integridad y los valores éticos de la organización, los parámetros que permiten llevar a cabo sus responsabilidades, es por ello que el ambiente de control se determina en función de la integridad y competencia de los miembros de la institución ya que este componente influye en la conciencia o conocimiento del control de cada persona.
2. Evaluación de riesgos: es el proceso mediante el cual se identifican y analizan los riesgos relacionados con el impedimento de los objetivos de la institución, para su estudio podemos considerar:
    a) Avances tecnológicos.
    b) Cambios operativos.
    c) Nuevas líneas de negocio.
    d) Personal nuevo.
    e) Reestructura, etc.
3. Actividades de control: son las acciones establecidas a través de políticas y procedimientos que contribuyan a garantizar que se lleven a cabo las instrucciones de Dirección para mitigar los riesgos con impacto potencial en los objetivos.

Según su naturaleza puede ser preventivos o de detección y pueden abarcar una amplia gama de actividades manuales y automatizadas, tales como:

2. Autorizaciones.
3. Verificaciones.
4. Revisión del desempeño empresarial.
5. Segregación de funciones, etc.

4. Información y comunicación: es el proceso continuo e interactivo de proporcionar, compartir y obtener la información necesaria. La comunicación interna es aquella que se difunde a través de toda la organización, esta debe de fluir a todos los niveles. Esto hace posible que el personal pueda recibir un mensaje claro de las responsabilidades de control que son obligatorias por parte de de la alta Dirección. También existe la información externa, esta persigue dos finalidades comunicar de fuera hacia el interior de la institución, información externa relevante y proporcionar información interna relevante de dentro hacia afuera en respuesta las necesidades y expectativas de nuestros clientes.

5. Sistema de supervisión y monitoreo: las evaluaciones continuas se utilizan para determinar si cada uno de los componentes de control interno, incluidos los controles para cumplir los objetivos de cada procedimiento funcionan adecuadamente. Los resultados se evalúan comparándolos con los criterios establecidos por los reguladores o la Dirección.

Nos centraremos en dos tipos de controles:

1. Control Mitigante: son acciones que reducen el riesgo, las cuales deben de ser bien planeadas y en el momento exacto del proceso para ser aplicado de manera directa.

2. Control compensatorio: no es aplicado de manera directa al proceso, ya que son acciones secundarias que ayudan a que personas ajenas al proceso lo contaminen, ayudando a robustecer el control mitigante.

1.3.2 Aplicación y monitoreo del control interno.

El control interno puede ser aplicado a todas las áreas de la institución con el fin de mitigar los riesgos existentes en cada uno de los departamentos, es de suma importancia mantener una correcta comunicación con el personal involucrado, proporcionarles capacitación continua, motivarlos, hacerlos sentir parte importante de la institución, crearles conciencia que forman parte de una gran cadena y que toda acción conlleva una reacción, ya que aquello que realizan pueden beneficiar o afectar su propio trabajo y en consecuencia a la institución, esto nos ayudará a robustecer nuestros procesos y considerar que tenemos una institución fuerte.

Monitoreo: es el mecanismo para evaluar el grado que cada control operacional, identificado si es eficaz, se realiza de acuerdo a como fue diseñado y si mitiga el riesgo al que está asociado. El monitoreo asegura que el control interno continúa operando efectivamente. [7]

Las herramientas de monitoreo deben de ser claras en su definición para obtener las alertas adecuadas que permitirán establecer acciones concretas, el alcance y la frecuencia del monitoreo deberá ser estipulado por Dirección ya que de ello dependerá los riesgos que se pretenden mitigar o eliminar.

El monitoreo nos permitirá conocer, si existen medidas de control que hagan la ejecución del proceso más lento y no sea efectivo para la institución, resaltará si los empleados están cumpliendo de manera adecuada los sistemas de control que fueron establecidos previamente.

[7] Mantilla Samuel Alberto / Control Interno: Informe COSO / Editorial ECOE Ediciones Cuarta Edición.

Es importante mantener una revisión continua y oportuna para detectar áreas de oportunidad y mantener la eficiencia en los controles. Las deficiencias del control interno deben ser reportadas a la Dirección informando los asuntos delicados para su respectiva toma de decisión para su corrección.

Controles claves que se pueden Implementar

1. Segregación de funciones.
2. Supervisión y/o revisión.
3. Autorización.
4. Conciliaciones y verificaciones.
5. Políticas corporativas.

1. Segregación de funciones: la división de funciones le permitirá al dueño de cada proceso a especializarse en sus tareas, conociendo aquellas afectaciones y riesgos implícitos al momento de efectuarse el proceso, así como también la manera de contrarrestarlos o prevenirlos.

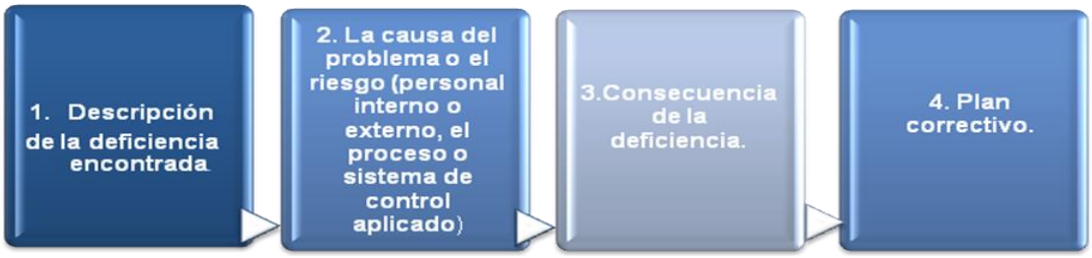
2. Supervisión y/o revisión: el área de control interno deberá de realizar una constante verificación del personal perteneciente a la institución, con la finalidad de validar que se esté cumpliendo de manera correcta con el proceso y la aplicación de cada uno de los controles establecidos en él.

3. Autorización: esta medida de control nos permitirá establecer una matriz con el nombre y facultades de aquellas personas dentro de la institución que podrán hacer uso de ellas de manera legal, operativa, etc., con la finalidad de que realicen toma de decisiones, siempre buscando el beneficio para la institución.

4. Conciliaciones y verificaciones: estos controles son más comunes en áreas contables y/o financieras ya que las conciliaciones diarias o mensuales que se efectúan en el departamento son un soporte de control que nos permitirá cerciorarnos que las transferencias y/o afectaciones a las cuentas fueron realizadas y registradas de acuerdo a lo proporcionado por el cliente o alguna otra área interna que haya enviado la instrucción.

5. Políticas corporativas: toda institución debe de contar con documentos previamente revisado y autorizado por el consejo administrativo, en el cual van implícitos todos los lineamientos a seguir dentro de la institución que deben de darse a conocer a cada uno de los integrantes para su respectivo cumplimiento.

El resultado obtenido durante el monitoreo permitirá realizar un informe en el cual se podrá dar a conocer a la Dirección los hallazgos encontrados como:

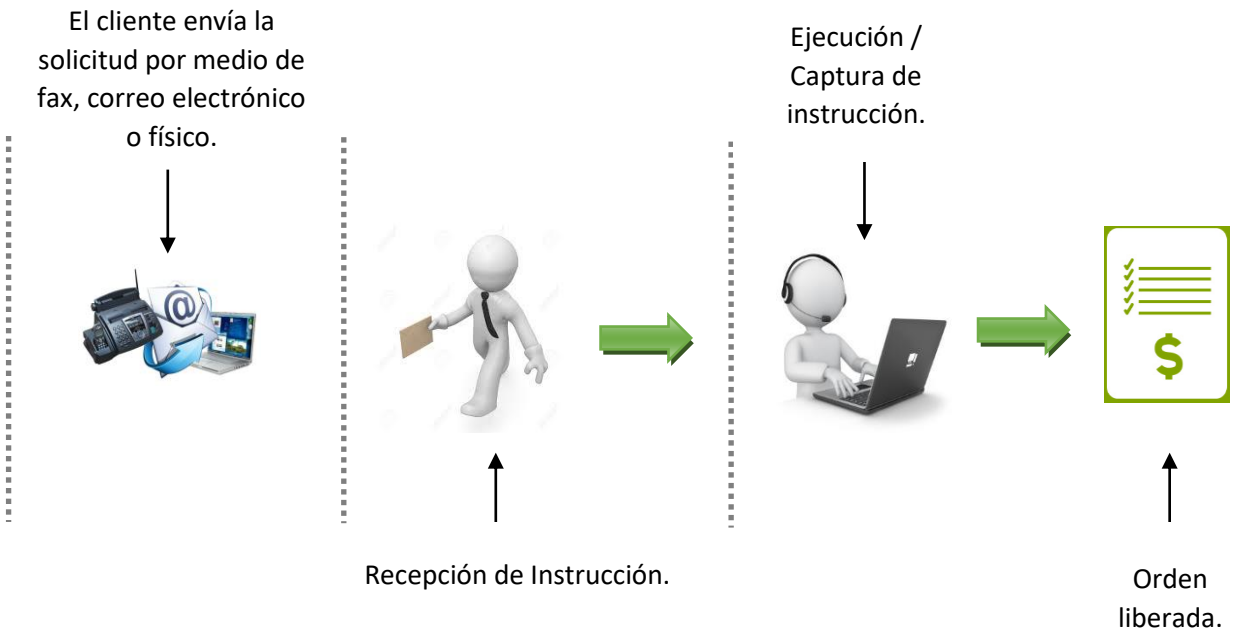


De esta manera el personal Directivo contará con un soporte formal y por escrito que le permitirá visualizar el estado actual de la institución, así como tomar aquellas decisiones pertinentes para el beneficio de todos.

Cuando existe un sistema de control interno efectivo, la alta Dirección y el consejo de Administración tiene una seguridad razonable de que en la estructura se llevan a cabo operaciones efectivas y eficientes; se preparan informes conforme a las regulaciones aplicables, teniendo la seguridad que cuenta con un personal capacitado para mitigar cualquier acción que ponga en riesgo a la institución.

A continuación, resumiremos el capítulo por medio de un ejemplo.

Proceso Fondeo de Cuentas.



El esquema anterior nos muestra el proceso de fondeo de cuentas, sin la existencia de control lo cual implica diversos riesgos hacia la institución y el cliente, por ejemplo:

1. Riesgo operativo: la persona encargada de capturar la información puede cometer errores y enviarlo a otra cuenta o no contar con las facultades correctas para afectar la cuenta, dejando en espera al cliente, o no realizando la instrucción.
2. Riesgo de fraude: la persona quien recibe la información del cliente puede crear una solicitud falsa o puede estar coludido con algún grupo externo para enviar dinero a cuentas propias.
3. Riesgo financiero: debido al riesgo anterior, la institución puede perder recursos económicos.
4. Riesgo regulatorio: al realizar una auditoria se podrá percibir la falta de controles y los riesgos que pueden perjudicar al cliente, lo cual ocasionaría que la institución sea acreedora a una multa.
5. Riesgo reputacional: el cliente tendrá una mala imagen de la institución al saber que sus operaciones no son seguras.

Implementación de Control Mitigante.

Envío de solicitud por medios certificados:

A) Fax.
B) Correo previamente autorizado.
C) Solo una persona debe entregar documento físico.
D) Formato debidamente firmado.

Segregación de Funciones

Maker / Checker

Maker

Ejecuta / Captura la instrucción.

Checker

Supervisa y evalúa la información capturada.

Call Back

Se realizará una llamada al cliente con la finalidad de confirmar su solicitud y visto bueno vía telefónica.

Explicación Implementación de Control Mitigante

En el esquema anterior se muestran un ejemplo de la aplicación del “Control Mitigante” que nos ayudará a contrarrestar el riesgo inherente que existe en el proceso y que fue especificado en el primer esquema.

Con el objetivo de contrarrestar los riesgos, se implementan ciertas acciones en el proceso que a continuación se enlistan:

1. Fax: el cliente contará con un número exclusivo de fax, perteneciente al departamento encargado del “Fondeo de cuentas” al cual podrá enviar su solicitud.

2. Correo previamente autorizado: la instrucción deberá de ser entregada a una dirección de correo electrónico, proporcionada por la institución el cual pertenecerá a la persona encargada del fondeo de cuentas.

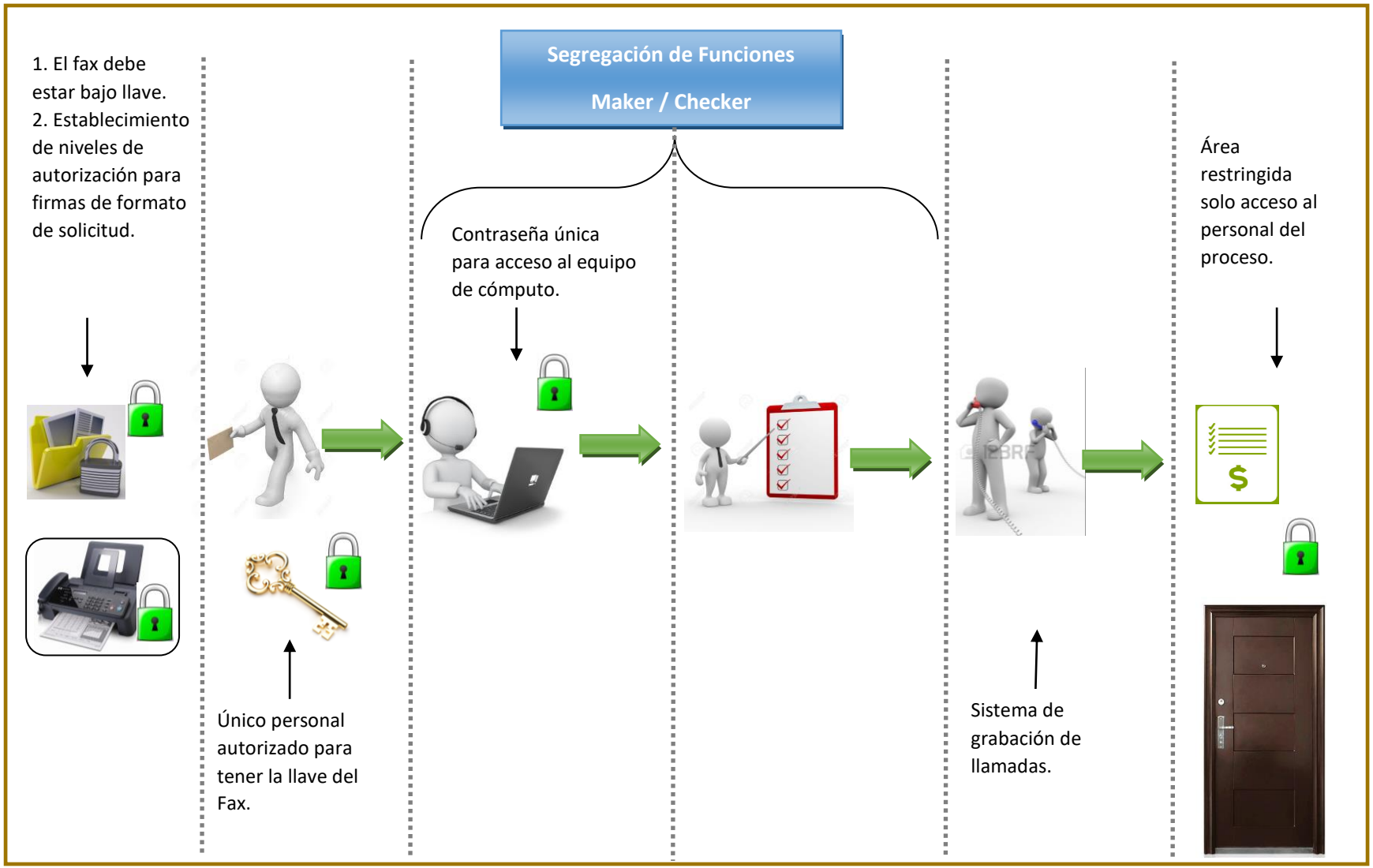
3. Entrega de documento físico: si es de predilección del cliente realizar sus transacciones de manera personalizada, deberá de dar a conocer a la institución el nombre de la persona facultada para hacer la entrega del documento físico. Así mismo la institución deberá de proporcionarle al cliente el nombre de las personas encargadas del fondeo de cuentas, las cuales deberán de pedir identificación a la persona que está entregando la documentación, con la finalidad de cerciorarse sea la indicada por el cliente.

4. Formato: la institución deberá de proporcionarle al cliente el formato que detallará aquella información necesaria para el fondeo de cuentas, dicho formato deberá de estar firmado por el cliente.

5. Segregación de funciones: permitirá dividir las actividades, mediante el “Maker y el Checker”. El maker será el encargado de llevar acabo la instrucción solicitada por el cliente, mientras el checker será el responsable de verificar que dicha ejecución realizada por parte del maker corresponda al 100% de lo solicitado mediante la instrucción del cliente.

6. Call Back: una vez realizada el fondeo de cuentas, deberá de efectuarse una llamada al cliente con la finalidad de verificar el cumplimiento de su solicitud y dar su visto bueno de común acuerdo.

Implementación Control Compensatorio.



Explicación Implementación de Control Compensatorio.

El esquema anterior nos muestra ejemplo de aquellos “Controles compensatorios “que se pueden implementar para mitigar los riesgos residuales en el proceso, ayudándonos a robustecer nuestros controles.

1. El fax deberá de encontrarse bajo llave, esto con la finalidad de que la información recibida se encuentre bajo resguardo seguro, y solo el personal autorizado pueda tener acceso a ella.

2. Establecimiento de niveles de autorización de firmas para el formato, en caso de que la persona encargada de firmar el formato solicitado se encuentre de vacaciones o incapacidad, deberá de establecerse previamente el nombre(s) de la(s) persona(s) que podrán firmar durante su ausencia.

3. Solo el supervisor del departamento encargado de fondeo de cuentas deberá de contar con la llave del fax, esto permitirá tener un control de acceso a la información.

4. El personal encargado del fondeo de cuentas deberá de implementar una contraseña única para el acceso al equipo de cómputo o sistemas, que no podrá ser compartida, con la finalidad que personal ajeno no pueda tener acceso a la información.

5. El sistema de grabación de llamadas permitirá contar con la evidencia correspondiente a la verificación con el cliente, quién deberá de confirmar que la transacción es correcta.

6. Restringir el acceso al área solo al personal involucrado en el proceso, evitará que gente ajena pueda escuchar o ver información pertinente al cliente, lo cual podría estar en riesgo.

Monitoreo de Control.

El área de control interno se encargará de validar el cumplimiento de control mitigante y compensatorio (Fax bajo llave, firmas autorizadas, etc).

Validación que solo el personal de recepción tenga llave.

Segregación de Funciones

Maker / Checker

Validación contraseña única para acceso al equipo de cómputo.

Validación segregación de funciones.

Solicitud de pruebas de grabación de llamadas.

Área restringida solo acceso al personal del proceso.

Capítulo 2 Seguridad de la Información.

2.1 Concepto de información y seguridad de la información.

Información: son aquellos datos procesados que tienen un significado o propósito, siendo de utilidad para la ejecución de procesos o la toma de decisiones.

Para Neil Fleming los datos se transforman en información añadiéndoles valor en varios sentidos, ya que son piezas importantes que representarán el entendimiento y conocimiento debido a su asociación en conjunto.

En una organización existen tres tipos de niveles del manejo de información:

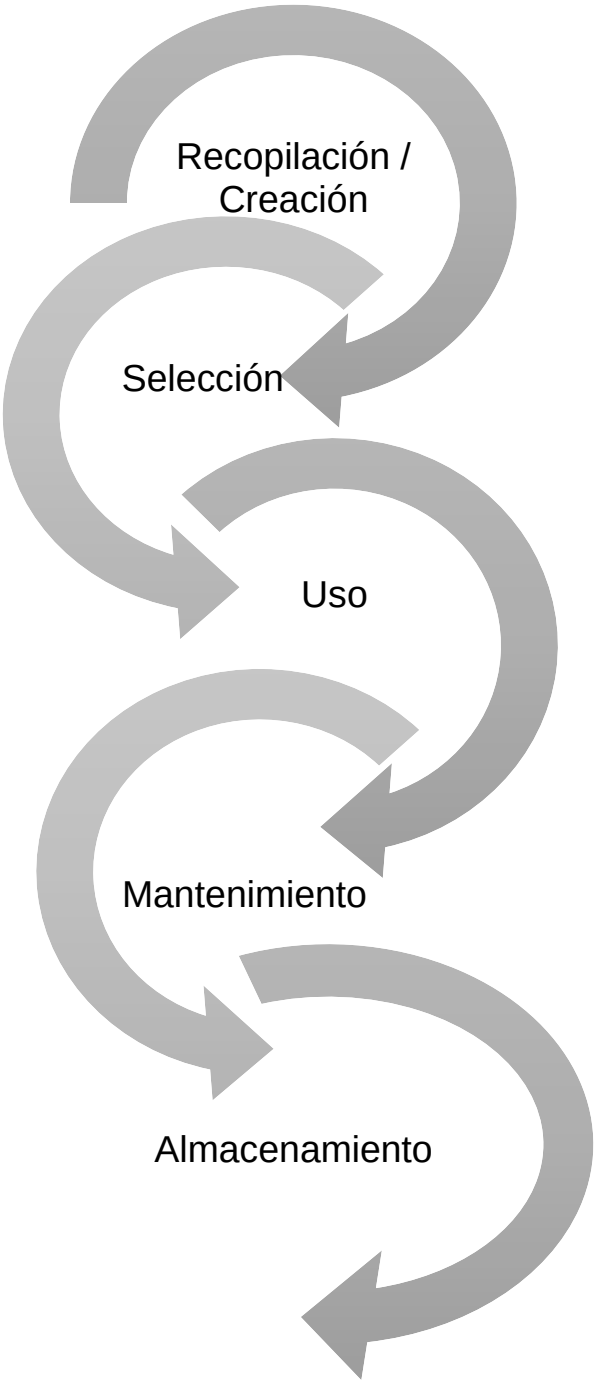
Nivel	Responsabilidad	Requerimientos
Estratégico	Planeación estratégica.	Más datos externos y subjetivos.
Táctico	Control administrativo.	Datos externos e internos.
Operacional	Control operativo.	Datos internos y objetivos.

Fuente Robert N. Anthony. Planning and Control System.

La información utilizada en estos niveles dependen unos de otros, ya que la información utilizada por los directivos para realizar la “Planeación Estratégica” en busca del crecimiento de la empresa, le proporcionará detalles a nuestro control administrativo para la implementación adecuada de los recursos humanos, monetarios, maquinaria, etc., a utilizar para cumplir los objetivo de la Dirección, resultado de ello ayudará al control operativo proporcionándole las tareas especificadas a realizar para cada área o persona de la manera correcta para el cumplimiento de sus objetivos.

La información debe considerarse como uno de los principales recursos de la empresa ya que de ella depende diversas actividades dentro de la institución incluyendo la toma de decisiones por parte de Dirección; por lo que deben implementarse controles para su respectiva seguridad y manejo adecuado, de ello dependerá el buen funcionamiento de la institución.

CICLO DE VIDA DE LA INFORMACIÓN.



1. Recopilación / Creación: es la obtención de información de los clientes, la cual se puede conseguir de diversas maneras:

a) Formatos por escritos.

b) Encuestas.

c) Buzón de quejas y/o sugerencias.

d) Entrevista.

e) Página de internet perteneciente a la institución.

f) Correo electrónico.

g) Teléfono.

2. Selección: la institución deberá de realizar un análisis de la información proporcionada por el cliente, con la finalidad de elegir aquella que será de utilidad para cada proceso.

3. Uso: es la aplicación de la información en el proceso.

4. Mantenimiento: la institución deberá de mantener constante comunicación con el cliente, con la finalidad de actualizar sus datos.

5. Almacenamiento: toda información ya sea digitalizada o física, deberá de contar con su respectivo resguardo, proporcionando seguridad y privacidad a la información del cliente.

La importancia de considerar nuestro ciclo de la información es respecto a la constante actualización y movilidad de objetivos en nuestra institución y las necesidades de nuestros clientes, ya que lo que hoy puede ser crítico para el negocio, con el tiempo puede dejar de tener importancia y disminuir su impacto de riesgo.

Los sistemas de información funcionan como herramientas de supervisión, recogiendo determinado tipo de datos de forma rutinaria, en otras ocasiones se toman acciones puntuales para obtener información. Los sistemas de información deben adaptarse para dar soporte a los objetivos de la institución.

La calidad de la información generada por los controles establecidos puede beneficiar o afectar la capacidad de la Dirección para tomar decisiones adecuadas al momento gestionar los procesos y sus resultados.

DIFERENCIA ENTRE RIESGOS, AMENAZAS Y VULNERABILIDADES EN LA INFORMACIÓN.

Debido a que el manejo de la información esta implícito en cada proceso es de suma importancia considerar que siempre estará relacionado el riesgo, que es aquella probabilidad de recibir un ataque que perjudique a la institución o algún proceso en particular, el riesgo nos indica lo que podría pasar a los activos si no se protegen adecuadamente.

La amenaza a diferencia del riesgo nos muestra el evento efectuado que puede generar un incidente o daños en la información.

La vulnerabilidad es aquella debilidad del activo que puede ser aprovechada para llevar acabo el ataque o amenaza. Es por ello de gran importancia implementar como medida de control la metodología “Seguridad en la información” la cual nos ayudará a mitigar los riesgos que pueden sufrir la información.

Seguridad de la información: son aquellos mecanismos, estrategias y acciones que permitan hacer realidad las metas operativas, previniendo ataques contra la confidencialidad, integridad y disponibilidad de la información.[8]

Según Russell Ackoff y Daniel Greenberg la seguridad de la información se concentra en la información y cómo debe de ser protegida, es decir, estudia sus detalles y medios de difusión o almacenamientos que permitan un acceso confiable y controlado.

Seguridad de la información: es el conjunto de controles, políticas cuyo objetivo es la protección de información mediante el correcto manejo y uso de ella. Cuando distribuimos datos de un cliente o de la misma institución esperamos que no se pierda y llegue al destinario correcto, cuando almacenamos documentación de suma importancia esperamos que no sea robada, es en estos casos y muchas otras posibilidades de riesgo que existen, la aplicación de seguridad de la información buscará prevenir y mitigar acciones que pongan en riesgo uno de los activos más importantes de la empresa.

Vicente Aceituno en su libro seguridad de la información, nos comparte la importancia de su implementación, ya que él considera la información como un activo perteneciente a la institución utilizado para realizar o mantener sus procesos.

Seguridad de la información según ISO 27001, se refiere a la confidencialidad, integridad, disponibilidad de la información y datos importantes para la organización, independientemente del formato que tengan, estos pueden ser: electrónicos, en papel, audio o video, etc.

[8] Cano Jeymi / Inseguridad de la Información una visión estratégica / Editorial Alfaomega.

BENEFICIOS DE SEGURIDAD DE LA INFORMACIÓN.

1. Se mantiene un ciclo de vida de la información controlado.

2. Concientización de los empleados.

3. Cumplimiento de legislaciones.

4. Se evitan sanciones, mediante el cumplimiento de marcos legales.

5. Mitigación de riesgos.

6. Mejora la competitividad del mercado, ya que se genera la confiabilidad con los clientes y proveedores, lo cual aportará a incrementar el prestigio de la institución.

El proceso de gestión de seguridad de la información se lleva a cabo a través de la combinación de instrumentos que el área de control interno deberá de aplicar en cada uno de los departamentos de la institución, con la finalidad de salvaguardar cada uno de los datos manipulados en los procesos; por ello es importante apoyarse de instrumentos en los cuales quede documentado su aplicación; por ejemplo:

1. Política de Seguridad: es una guía de acción a seguir, en el cual se describe los objetivos y estrategias definidas para la protección de la información perteneciente a la institución, especificando las obligaciones de los miembros de cada departamento. Dicho documento es revisado y avalado por áreas directivas y de control interno, dando a conocer ¿Qué se tiene que proteger? ¿De quién? y ¿Por qué?

2. Norma de Seguridad: deberá ser consistente con la política, la diferencia entre ella es que la norma es una acción en específico que ira dirigida a una función o departamento, ayudándonos a describir el ámbito de aplicación con las siguientes preguntas ¿Dónde? y ¿Cuándo?

3. Estándar de Seguridad: en el encontraremos los parámetros de controles que serán aplicados, especificando cuando y quién debe de realizar las actividades siguiendo el procedimiento de seguridad.

4. Procedimiento de Seguridad: es el documento en el cual encontraremos el flujo de la manera en que se realizarán el conjunto de actividades implementadas como control para resguardar la información.

5. Plan de continuidad de operaciones: es aquella estrategia que como su nombre lo dice busca dar continuidad a las actividades y/o servicios ofrecidos al cliente por medio de un plan alternativo, en el caso de que la institución llegue a tener algún ataque, esta estrategia podrá permitir definir un esquema de comunicación alterno hacia nuestros empleados, clientes y proveedores en caso de un evento de crisis, con la finalidad de contactarlos previniéndolos de no proporcionar ninguna información por medio de teléfono, correo electrónicos, etc.

Los documentos mencionados anteriormente nos ayudarán a tener indicadores y métricas que nos permitirán evaluar los objetivos de seguridad establecidos.

Los principales objetivos de seguridad de la información son:

1. Integridad: garantizar que la información proporcionada, no haya sido alterada, eliminada o manipulada por personal no autorizado.

2. Confidencialidad: hace mención al manejo de la información confidencial o restringida que no sea revelada a personal no autorizado, la aplicación de dicha protección debe de ser utilizado para cualquier método de manejo digital, en papel o personal, esto conlleva el control de acceso a la información ya que se dará estas facultades únicamente al personal autorizado.

3. Disponibilidad: es aquella condición de que la información se encuentre a disposición del personal autorizado para su correcto uso o consulta de ello en el momento que lo requieran, ya sea por medio de sistemas tecnológicos o papel.

4. Confiabilidad: es aquel sentimiento de garantía que podemos proporcionar hacia los clientes, asegurándoles que su información se maneja bajo ciertos estándares de control que los mantienen protegidos.

5. Herramienta principal para la toma de decisiones.

Las principales responsabilidades de seguridad de la información en materia de control interno son:

1. Implementar procesos y elementos tecnológicos apropiados con el fin de lograr que existan controles que salvaguarden los activos de información de cada área.
2. Evaluar los riesgos de seguridad de la información que existen en cada una de las áreas de la institución.
3. Coordinar el proceso de elaboración y aprobación de entrega de información a personal externo.
4. Coordinar pruebas de vulnerabilidad en aplicaciones de internet a las cuales pueden acceder los empleados.
5. Proporcionar materiales de capacitación a todos los niveles de la institución con el objetivo de que tengan conocimientos en seguridad de la información.

Para una correcta aplicación de seguridad de la información existen 3 elementos principales que deberán de ser analizados, debido a la relación que tienen entre si para la ejecución de los procesos, implicando los riesgos que pueden existir entre ellos, el análisis de cada uno nos permitirá la aplicación de los controles necesarios para mitigar los riesgos.

1. Información, cualquier tipo de datos que tengan relación entre la institución, empleados, clientes y proveedores.

2. Equipos de cómputo pertenecientes a la organización, considerando software y aplicaciones necesarias para la ejecución de procesos.

3. Usuarios, considerando a cada una de las personas que interactúan para la obtención y manipulación de la información.

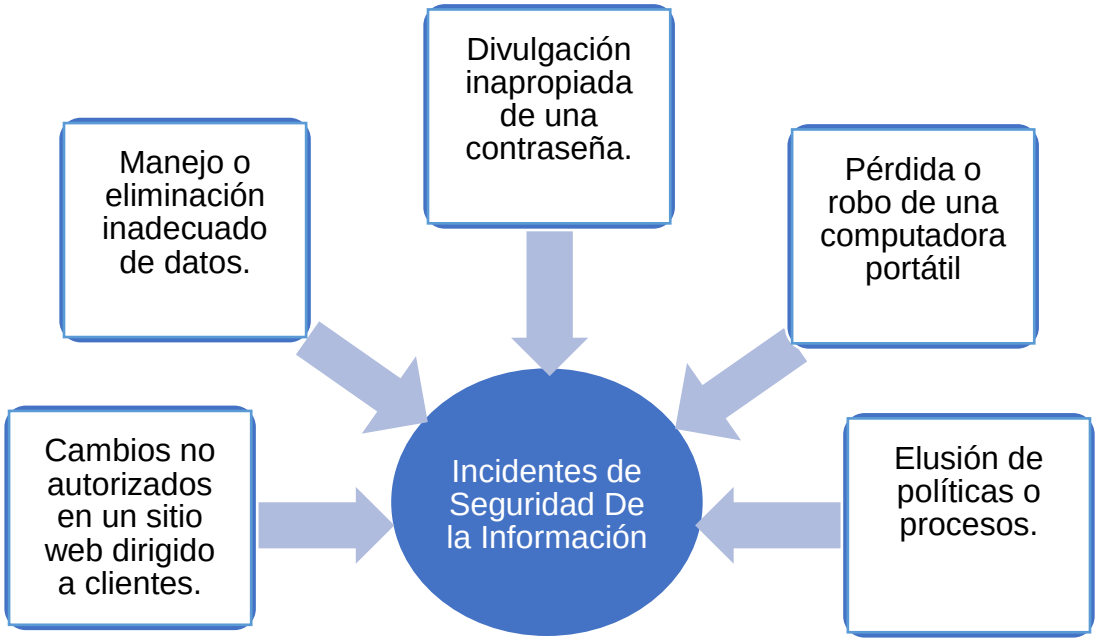
Cualquier medida de seguridad puede llegar a tener un defecto, es por ello la importancia de conocer y aprender a detectar que es un incidente de seguridad de la información.

Un incidente de seguridad de la información es cualquier evento que de forma accidental o intencional dañe, altere, destruya o provoque la divulgación, pérdida o robo de información, datos de la institución. Algunos de los factores que vuelven propenso un incidente puede ser cuando los empleados tienen cierto grado de confiabilidad en lo que realizan, se sienten protegidos por la antigüedad y/o durabilidad que llevan realizando su proceso ya no lo toman como una especialización, lo empiezan a observar de manera monótona, lo cual implica un riesgo, esto debido a que le impedirá visualizar los riesgos implicados, ya que su estado de alerta y previsión se encuentran disminuidos por la zona de confort, lo llevará a tomar acciones que ponen en riesgo los datos manejados en sus actividades; otro factor que provoca un incidente es la nula o mala información proporcionada a los clientes y empleados ya que pueden actuar con cierta naturalidad sin saber que existe una reacción que perjudique su estabilidad.

Es por ello que la institución debe proporcionar de manera continua capacitación a los empleados creándoles un grado de concientización de la importancia que es manejar y resguardar la información, así como darles a conocer todos los riesgos externos e internos que amenazan su proceso día a día, los cuales siempre serán muy variantes ya que las amenazas no siempre atacarán por el mismo lado, de esta manera se genera un poco de incertidumbre al momento de manejar la información llevándonos a tomar acciones más conservadoras y conscientes de cada paso que damos.

Como mencionamos en el capítulo anterior los controles deben de ser implementados en todas las áreas de la institución y a todos los niveles; es decir desde el nivel directivo hasta cada uno de los subordinados, recordemos ciertas acciones se dan en cadena; es decir si los niveles directivos no muestran interés en la protección de la información que se maneja en la institución por consecuencia los empleados no tomaran el respectivo cuidado y control de lo que los datos de su proceso conlleva, en cambio si los directivos están consientes de todo lo que fluye en la institución y comunican a sus subordinados que la información es un activo crítico y sensible que debe de ser protegido y manejado con los controles adecuados, generarán empleados más preventivos y una cultura de seguridad de la información que nos ayudará a crear una institución protegida y confiable.

Ejemplos de Incidentes de Seguridad.



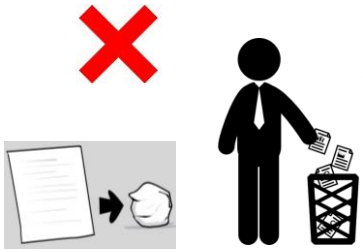
PRÁCTICAS SOCIALES QUE PONEN EN RIESGO LA INFORMACIÓN.

Una de las amenazas más sencilla pero impactante es la naturaleza de confiar en los demás y dejarnos ir por la sensación de confianza y amistad que una persona puede influenciar sobre otra, influyendo en las acciones a tomar.

A continuación, se enlistan aquellas acciones naturales que realizamos sin generar la conciencia del riesgo que implican.

1. Dumpster Diving: es aquella persona que está mirando a través de los contenedores de basura de la oficina para encontrar información que puede ayudar en el fraude, robo de identidad u otros tipos de actividad criminal. Al momento de desechar la información en muchas ocasiones no se presta la mayor importancia, por lo cual no se tiene conciencia de que también existe riesgo en ello, ya que la mayoría de las veces al desechar un estado de cuenta, contraseña o algún documento con información personal, generalmente el documento es compactado o destruido rompiéndolo solo en dos partes, ignorando el riesgo, ya que existen personas enfocadas a recuperar los pedazos de papel desechados, con la finalidad de armarlos para poder obtener los datos importantes del documento y hacer uso de ellos.

Es por ello de gran importancia crear concientización a los empleados de esta práctica, tomando como ejemplo, una medida de control el uso de trituradora de papel; ya que esta herramienta ayuda a destruir gran parte de la información, haciendo más difícil al defraudador el poder armar el documento. Debemos tomar en cuenta que esta práctica no solamente es con información en papel, también podemos desechar equipos de cómputo viejos, USB, discos, etc. Dando pauta a que la información pueda ser recuperada por las personas encargadas de esta modalidad de fraude, por lo cual es recomendable borrar toda la información antes de ser desechado el material.



2. Conversaciones en lugar público: ocurre en los ascensores, vestíbulos de los edificios o restaurante, se recomienda no discutir información relacionada con el trabajo (especialmente información confidencial) con los colegas del trabajo ya que nunca se sabe si alguna persona ajena está prestando atención a la conversación con el objetivo de realizar algún acto malicioso en contra de la institución. Es muy común que durante la hora de comida o al término de la jornada laboral, vayamos en compañía de nuestros colegas conversando al respecto de nuestras actividades suscitadas durante el día, si hubo algún problema con un cliente, si existe un proyecto de producto nuevo que será lanzado al mercado, alguna fusión con otra compañía etc. En muchas ocasiones estamos tan enfocados en nuestra conversación que no se puede percatar si existe a nuestro alrededor alguna persona perteneciente a la empresa competidora, algún defraudador, etc. Que pueden tomar ventaja de la información escuchada, teniendo datos que pueden ser usados en contra de la institución, el cliente, o hasta del mismo personal, es inevitable no contar los sucesos de nuestro día con nuestros compañeros, pero podemos concientizar al personal a que toda información deberá de ser conversada en lugares apropiados, es decir, oficinas y sala de juntas.

3. Masquerading: es aquella persona que está pretendiendo ser otra para obtener acceso legítimo a información autorizada. Si alguien pide información personal o de la institución hay que asegurarse de saber quién es, a que área pertenece, si tiene derecho a la información antes de proporcionar cualquier dato. La práctica más común para ello es de manera informática, cuando el defraudador consigue la contraseña y nombre de usuario de la persona que tiene acceso a la información, con la finalidad de ingresar y poder observar los datos que maneja, ejemplo de ello, llamadas de falsos ejecutivos en nombre de la institución realizadas a clientes, en la actualidad es muy común el enmascarase vía telefónica, una persona fingiendo ser ejecutivo del banco realiza llamada a un cliente, indicando que se está realizando cierta compra y si está de acuerdo de que el banco ejecute el pago, al momento de que el cliente dice que no realizó dicho compra, el personaje suplantador le solicitará información de su cuenta para poder acceder y cancelar el cargo no reconocido, es por ello de gran importancia que la institución financiera mantenga constante comunicación con su cliente para prevenirlo de este tipos de actos, en los cuales le debe de indicar que nunca debe de proporcionar su número secreto, para ello los bancos han implementado controles compensatorios como:

a) Notificaciones como mensajes a su número de celular previamente proporcionado al abrir su cuenta, con la finalidad de que, al momento de realizar una compra, llegue un mensaje de texto a su celular indicando el monto de la compra, fecha, lugar y hora.

b) Notificaciones vía correo electrónico, teniendo la misma funcionalidad que el método anterior.

4. Piggybacking: ocurre cuando una persona autorizada le concede a otra no autorizada el acceso a un área segura, el acceso a área restringida es controlado por su credencial, el permitir el acceso a persona ajena pone en riesgo la información. Quizás el acceso a otra persona no es intencional, sin embargo existen escenarios que pueden facilitar que una persona ajena acceda al lugar, por ejemplo ejecutivos en una sucursal bancaria que tienen acceso a cajas deben tener controles para asegurar su acceso seguro, uno de ellos cuidar que al momento de digitar su clave de acceso no exista persona cerca que pueda visualizar la clave, para después ingresar, también deberá tener el cuidado de que no haya persona a su lado que pueda empujarlo al momento de que la puerta se abra e ingrese junto con el ejecutivo.

5. Shoulder surfing: ocurre generalmente en espacios públicos o transporte público cuando un extraño intenta observar la información que se ingresa en una computadora tratando de mirar por un costado. En la actualidad diversas compañías están poniendo en práctica el modelo de Home Office o “trabajo en casa” este método permite que el empleado pueda conectarse vía remota a la institución para poder realizar sus labores, es por ello indispensable crear consciencia a los empleados que trabajan bajo esta modalidad, que el lugar en donde se encuentre sea seguro, es decir no conectarse en espacios públicos como restaurantes, cafeterías, transporte público, parques, etc. Debido a que ello implica un riesgo ya que puede existir alguna persona a su lado que esté tratando de mirar por encima de su hombro, y tener visualización y contexto de la información que maneja la persona, poniendo en riesgo a la institución o al mismo empleado ya que puede ser atacado para tener la información en cuestión.

6. Suplantación de identidad: es el uso de correos electrónicos o anuncios fraudulentos diseñados para engañar al destinatario con la finalidad de que revele su información por medio de algún documento o vía tecnológica ingresando a algún link proporcionado por el suplantador.

2.2 Clasificación de la información.

La información manipulada en cualquier institución siempre existirá un grado de vulnerabilidad de recibir un ataque interno o externo que aproveche la situación perjudicando a la institución, a sus empleados o clientes, es por ello de gran utilidad realizar la clasificación de información, ya que nos permitirá determinar directrices que estipularán de que manera se debe de proteger la información con la que se está trabajando, sin importar el formato que utilicemos, pudiendo ser de manera digital o en papel, si su uso será solamente para almacenamiento, transmisión, eliminación, etc.

No toda la información tiene la misma importancia para la institución, ni puede generar los mismos impactos en caso de ser atacada, por ello es importante realizar una valoración y/o análisis de la relevancia que tienen y los impactos que generarían; cualquiera que sea la clasificación estipulada por la institución deberá de implementarse controles para su manejo; cabe mencionar que cuanto mayor sea el grado de importancia y sensibilidad otorgada a la información, los controles deberán de ser más estrictos.

Definiremos la clasificación de la información como el proceso de evaluar y categorizar la información por nivel de riesgo asociado para que pueda manejarse en consecuencia. Los niveles de clasificación proporcionan orientación para determinar cómo proteger la información basada en su formato (por ejemplo, digital, papel, etc.) y el uso previsto (por ejemplo, almacenamiento, transmisión etc.).

Cuando realizamos una clasificación o segmentación de la información, se le está asignando cierto nivel de importancia y de protección, de esta manera nos aseguramos de que el empleado tiene el conocimiento necesario para el correcto manejo de los datos recibidos.

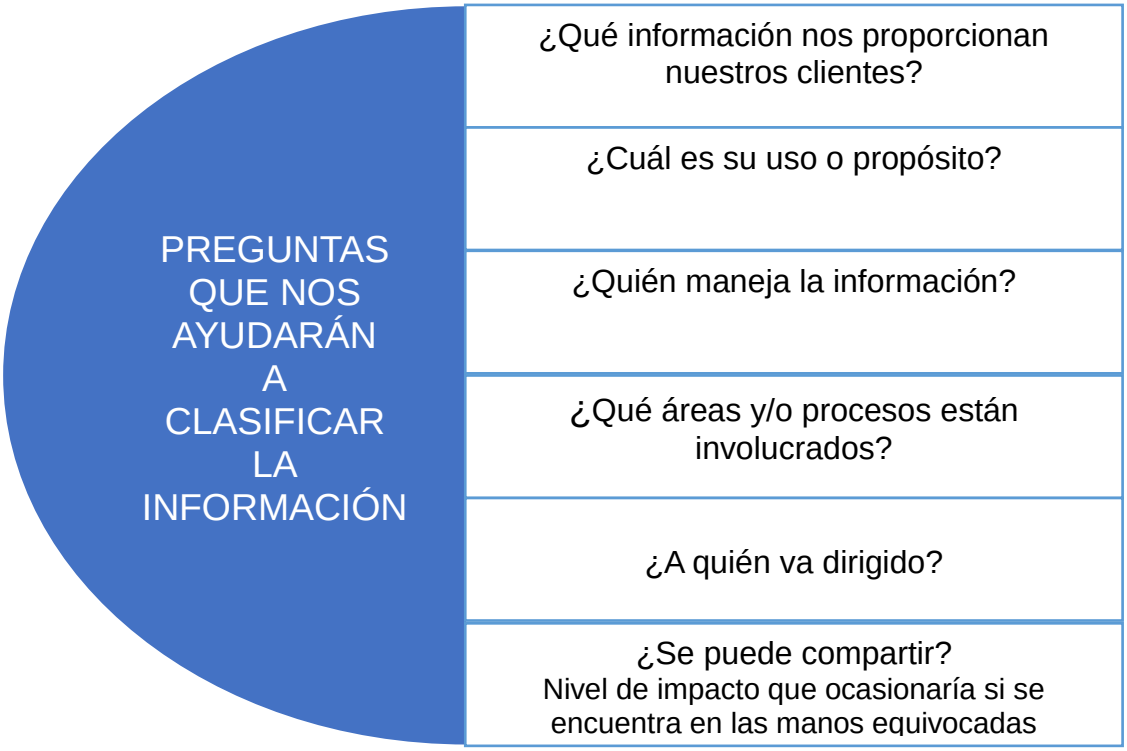
PRINCIPALES OBJETIVOS DE LA CLASIFICACIÓN.

1. Garantizar que la información cuente con un apropiado nivel de protección.
2. Identificar, señalar la sensibilidad y su criticidad.
3. Proteger su integridad.
4. Definir los controles a implementar de acuerdo con los niveles o clasificación estipulada.

BENEFICIOS.

1. Identificación de la información sensible y vital.
2. Identificación de los propietarios y responsables de su manejo.
3. Establecimiento de control de acceso.
4. Reducción del riesgo de pérdida, robo o corrupción de información.
5. Reglas claras para el personal de la organización.
6. Aumento de seguridad.

Si en una organización no se utiliza esta práctica, toda información se manejaría de la misma manera; el empleado y /o cliente no tendría conocimiento de que datos pueden ser compartidos al público en general y cuales deben de contar con cierta restricción para su protección, aumentando la posibilidad de incidentes de seguridad, generando riesgos legales, reputacionales, financieros, de fraude etc.



El correcto análisis y clasificación de la información nos proporcionarán las directrices para determinar los controles que se pueden aplicar para su resguardo y protección con la finalidad de mitigar los riesgos implícitos. La clasificación de la información debe de ser documentada por el propietario, aprobada por la gerencia y distribuida a todo el personal. En caso de existir algún cambio al tipo de información solo el propietario podrá hacerlo, mediante una justificación aprobada por la gerencia y la revisión con el área de control.

La institución deberá de contar con un documento ya sea procedimiento o política, en el cual se encuentre estipulado la clasificación de su información y el manejo de cada una de ellas, esto con la finalidad de darlo a conocer a cada uno del personal involucrado de esta manera podemos garantizar que tendrán el conocimiento adecuado para su manejo el cual ayudará a mitigar los riesgos. Es importante que al empleado le quede claro lo que está realizando y porque, con ello existe la transparencia al proceso e involucramos al personal, ya que generamos el sentimiento de pertenencia en sus actividades, elevamos su motivación al sentirse parte esencial de la institución y a la importancia que tiene sus actividades, de esta manera logramos que realice sus funciones de acuerdo con la normatividad y los controles establecidos.

2.2.1 Pública.

Es información disponible libremente fuera de la institución que está destinada a la distribución interna y externa, por ejemplo:

a) Informes anuales.

b) Nombre de contactos.

c) Horarios de servicio.

d) Productos en sitios web.

e) Comunicados de prensa.

2.2.2 Interna.

Es información comúnmente compartida dentro de la institución, pero no está destinada para la distribución externa, por ejemplo:

a) Procedimientos operativos.

b) Políticas.

c) Estándares.

d) Materiales de capacitación.

2.2.3 Confidencial.

Es información que la institución está obligada a proteger, por ejemplo, información perteneciente a clientes, trabajadores. Esto puede incluir cualquier combinación de datos sujetos a restricciones regulatorias o contractuales sobre divulgación, así como información que la institución determine que tiene el potencial de proporcionar una ventaja competitiva o un impacto significativo en el negocio si se revela a personas no autorizadas. Incluyendo datos de nómina y compensaciones, posiciones, comercio e instrucciones de movimiento de efectivo, informes de auditoría y estrategias de marketing.

Este tipo de información debe de ser almacenada en dispositivos pertenecientes a la institución.

2.2.4 Confidencial de identificación personal.

Identificación personal: cualquier información acerca de un individuo gestionada por una agencia que puede ser usada para distinguir o seguir la identidad de una persona.[9]

Información que identifica a una persona, la cual se considera confidencial ya que de ser publicada pondría en riesgo la privacidad y seguridad de la persona en cuestión, facilitando el robo de identidad, fraude de crédito u otro fraude financiero.

Ejemplos:

a) Nombre de la persona.

b) Dirección, teléfono o dirección de correo electrónico.

c) Número de pasaporte.

d) Número de licencia de conducir.

e) Número de identificación del cliente (núm. Tarjeta de crédito, débito, identificadores de cuentas que pueden resultar en movimientos de fondos u otro número de cuenta financiera)

f) Número de seguro social.

Dicha información la institución la considera como uno de los activos más importantes que debe de recopilar, usar y proteger como el dinero, ya que implica la seguridad de los clientes es por ello que todas las instituciones manejan la estrategia de “Privacidad de la Información”.

Privacidad: se refiere a la recopilación justa, ética y legal, al uso compartido y disposición de la información personal.

Privacidad: el derecho de una persona a controlar la información acerca de si misma y la recopilación, uso, intercambio y eliminación de información personal de manera justa, ética y legal.

La privacidad también incluye los derechos y las obligaciones de las personas con respecto a cualquier uso de su información confidencial identificable.

1. El derecho de proporcionar su información y permitir que la institución controle los datos necesarios para el proceso.

2. La capacidad de controlar cómo es identificado, localizado y contactado.

3. Los derechos y obligaciones de las personas con respecto al uso, divulgación y retención de su información personal.

[9] National Institute of Standard and Tecnology.

Este programa o estrategia permite ganar la confianza del cliente, al saber que su información se encontrara protegida y será solamente utilizada para los fines que el autorice. Recordemos que la privacidad de la información está regulada, siendo un requerimiento legal y normativo que toda empresa debe de cumplir, con la finalidad de tener protegido al cliente e informado de que la información proporcionada será almacenada por la institución.

2.2.5 Restringida.

Es aquella información que si se revela a personas no autorizadas puede tener un impacto negativo significativo en las obligaciones legales o reglamentarias de la institución en su situación financiera, clientes o franquicia, incluida su reputación como una institución financiera de confianza, por ejemplo:

a) Datos importantes como fusiones y adquisiciones antes de la divulgación pública.

b) Documentos de estrategia ejecutiva.

c) Informes financieros antes de la divulgación pública.

2.3 Controles dentro de la seguridad de la información.

2.3.1 Segregación de funciones.

El área de recursos humanos es el encargado de realizar estudios de antecedentes apropiados al personal que sea reclutado, así mismo debe de informar al personal los sistemas información creada, enviada, recibida, almacenada y procesada. Esta área es de gran apoyo, debido a que cuentan con el documento oficial de descripción de puesto, el cual especifica:

1. Propósito de puesto.
2. Responsabilidades del puesto.
3. Actividades a realizar.
4. Perfil del empleado.

Ello nos ayudará a tener documentado las diversas funciones existentes en la institución, proporcionándole apoyo al área de control, con la finalidad de que cuente con el conocimiento del perfil y funciones correspondientes a cada persona.

La concentración de funciones en una sola persona aumenta el riesgo de errores en el proceso por la falta de existencia de supervisión, o aumenta el riesgo de fraude; por ejemplo:

a) Documentación falsificada.

b) Pagos indebidos.

c) Transferencia de fondos a cuentas personales.

d) Baja de cuentas por cobrar indebidamente.

e) Autorización de servicios a clientes, fuera de política.

f) Emisión de reportes financieros ficticios.

Segregación de Funciones: esta relacionada con la asignación a personas distintas las responsabilidades de autorizar transacciones, registrar operaciones y mantener la custodia de activos, que podría reducir las oportunidades que cualquier empleado oculte errores o perpetré en fraude.[10]

Las responsabilidades se dividen o segregan, entre diferentes empleados para reducir el riesgo de error o acciones inapropiadas. La segregación de funciones debe de garantizar la independencia de las funciones de cada persona, de esta manera podríamos generar la segregación primordial "Maker – Checker" (operador y autorizador).

Derivado de ello deberá de realizarse la división de responsabilidades, estipulando los poderes y/o facultades que cada persona tendrá para la realización de sus funciones.

Ninguna persona deberá tener demasiadas facultades para manipular un sistema que le permita ejecutar transacciones en todo un proceso de negocio sin controles ni autorizaciones, por ejemplo:

a) Un individuo que es encargado de generar transacciones no debe tener las facultades para autorizar o generar conciliaciones contables.

b) La persona encargada de autorizar transacciones no deberá de tener acceso al sistema de captura de ellos y/o modificación de la información.

Toda actividad debe de pasar por un proceso de:

1. Solicitud.
2. Ejecución.
3. Aprobación.
4. Registro.

[10] Fonseca Luna Oswaldo / Sistemas de Control Interno para Organizaciones / Editorial IICO.

Esto nos ayudará a la realización correcta y segura del proceso, evitar errores involuntarios, fraudes, desfalcos, etc.

La segregación de funciones es una medida de control que nos permitirá reducir el riesgo de errores y fraudes mediante la aplicación de la división de tareas entre los empleados.

Para ejemplificar esta medida de control, retomemos el proceso del capítulo 1 “Proceso Fondeo de Cuentas”

En el diagrama anterior podemos observar la división de funciones en 2 esenciales roles (obsérvese la cuadricula punteada en color rojo) “Maker y Checker”.

Maker es el operador encargado de llevar acabo la ejecución de la transacción solicitada por el cliente; mientras el checker será el verificador y aprobador; en el ejemplo anterior podemos visualizar que en el mismo proceso se ejecuta dos veces las funciones de checker, una de ella es al momento de validar que la ejecución por parte del maker se haya efectuado de acuerdo a lo solicitado por el cliente de manera correcta y oportuna, la otra implementación es en el callback el cual se hace una verificación y/o validación con el cliente respecto al monto a transferir, esto con la finalidad de robustecer nuestro proceso y mitigar el riesgo. De esta manera evitamos que una sola persona tenga diversas funciones en el mismo proceso e incremente el riesgo de fraude por ejemplo en el caso anterior, el maker NO podría contar con las siguientes funciones:

a) Asesorar inversiones.

b) Aprobar créditos.

c) Administrar documentos.

d) Custodiar Tarjetas de firmas.

e) Emitir estados de cuenta.

f) Modificar sistemas.

Ya que si contará con estas funciones se autogestionaría y existiría el mayor porcentaje de riesgo de fraude al no tener alguien que supervise sus actividades.

La función de checker debe de asegurar que todos los requisitos de control que correspondan a la transacción se hayan cumplido antes de efectuar el movimiento de fondos.

Algunos ejemplos son:

1. La documentación proviene de una fuente autenticada.
2. Los detalles de la transacción en el sistema concuerdan con la solicitud.
3. El callback se llevó a cabo de forma satisfactoria.
4. Las firmas de la instrucción concuerdan.

Todos los errores de ingreso en el sistema que el checker identifique deben de devolverse al maker (quien ingresa los datos) o se debe de solicitar un aprobador alternativo en caso de que el mismo checker realice la corrección, esto para evitar la colusión del maker y checker para un fraude.

Es importante considerar la aplicación de niveles adicionales de revisión y aprobación cuando la transacción implique mayor exposición.

Maker	Checker
Responsable de la acción inicial	Comprueba la exactitud y autenticidad de la acción inicial, usando los datos fuentes.
Responsable de la autenticidad y aplicación de la actividad o función.	Tiene mayor grado de experiencia que el Maker. Tiene mayor conocimiento de la función.
	Certifica que el maker ha llevado a cabo sus funciones y controles de manera adecuada.

REQUISITOS PARA LA SEGREGACIÓN DE MAKER CHECKER.

1. El “Maker y Checker**”** deberán de tener claros los objetivos y riesgos que implican su proceso.

2. Ninguno de los dos podrá auto gestionarse ante la ausencia de alguno, es decir el maker no podrá aprobarse a si mismo las transacciones realizadas, y el checker no podrá realizar correcciones en el sistema, en caso de algún error deberá de ser corregido por el maker.

3. Deberán de mantener una constante capacitación, ante los diversos riesgos en su proceso y qué acciones tomar para mitigarlos.

4. Comprender su nivel de responsabilidad, para efectuar el proceso con integridad, exactitud y autenticidad.

5. Contar con los conocimientos de las políticas que rigen para la elaboración de su proceso.

6. El Maker y el checker deben asegurarse de que se han cumplido todos los requisitos de control para las transacciones (la información requerida para la documentación legal / regulatoria es de una fuente autenticada, los detalles de la transacción en el sistema están de acuerdo con la solicitud del cliente, las firmas concuerdan con los registros del archivo) antes de ejecutar y/o completar la tarea.

7. El checker es responsable de asegurar que existe documentación de soporte adecuada para evidenciar correctamente la autenticidad y exactitud de la transacción.

2.3.2 Control de acceso a la información.

Para ciertos procesos en los cuales se vea implicada información restringida se deberá de considerar accesos controlados o la implementación de zonas reservadas en las cuales, solo el personal autorizado pueda tener acceso a ella, la finalidad del control de acceso es que un usuario sea identificado y autentificado de manera detallada y segura para que le sea permitido el acceso.

El control de acceso a la información disminuirá el riesgo de distribución de la información, el impedir acceso a la información manejada en una institución a aquellas personas que no pertenezcan a ella o que no tengan relación alguna con el proceso, evitaría el riesgo de pérdida o distribución de la misma.

PRINCIPALES OBJETIVOS:

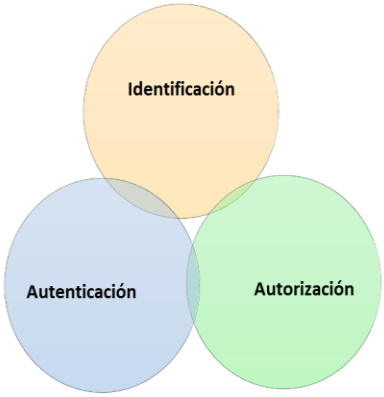
1. Impedir acceso no autorizado a los sistemas de información, base de datos, documentos, equipos de cómputo, etc.

2. Implementar seguridad.

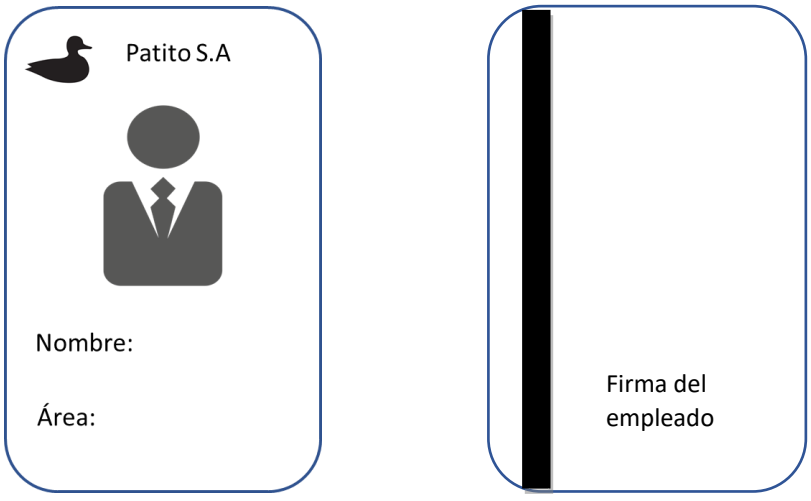
3. Concientizar a los empleados respecto a su responsabilidad en el resguardo y manejo de la información implícita en su proceso.

4. Salvaguardar la información confidencial de la institución o del cliente.

Este tipo de control puede ejecutarse de acuerdo con los niveles de seguridad que se requieren implementar por la información que se maneje en dicho departamento, zona o equipo de cómputo, para ello consideremos 3 métodos generales como control de acceso:



1. Identificación: son aquellos métodos en los cuales el empleado utiliza alguna herramienta en el cual se pueda corroborar por medio de la combinación datos y rasgos físicos quien es. El ejemplo más común es la asignación de credencial, la cual le da acceso a la institución, pero también puede ser configurada para permitir acceso a alguna área en específico.

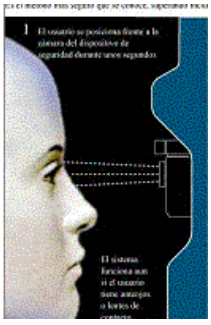


En la actualidad la utilización de una credencial como identificación ya no es 100% segura, debido a los avances tecnológicos, se ha facilitado la falsificación de ellas, o también existe la posibilidad del robo o extravió por parte del empleado, por ello la importancia de ir actualizando los métodos de seguridad, algunas empresas el día de hoy utilizan la huella digital como acceso de control.

2. Autenticación: este método es un sistema de control más robusto debido a que el reconocimiento del personal es más específico y seguro debido a el control de acceso por “Biometría” este conjunto de herramientas permiten distinguir al personal mediante la utilización de rasgos físicos del empleado que no pueden ser suplantados con facilidad, por ejemplo:

a) Acceso por reconocimiento de voz, esta tecnología tiene la finalidad de identificar al empleado por medio de su voz.

b) Reconocimiento de iris: este control es ocular, para que el empleado pueda tener acceso al área, será necesario que coloque su rostro frente al equipo el cual leerá los rasgos del iris, si coincide será permitido el acceso.



c) Huella dactilar: es el método biométrico más común en las instituciones, para ello el empleado deberá colocar un dedo en el aparato, el cual identificará los rasgos de la huella del empleado, si ello coincide permitirá el acceso al empleado.

3. Autorización: este método depende en ocasiones de una tercera persona, por ejemplo, en algunas instituciones al llegar una persona ajena del edificio, así sea de la misma compañía es necesario que la persona a quien va a visitar envíe un correo con el visto bueno al equipo de seguridad del edificio para que permitan el acceso a la persona.

Independientemente de los métodos mencionados anteriormente, consideremos métodos de control compensatorio que nos ayuden a robustecer el acceso a la información. Recordemos que los empleados pueden tener acceso a diversos sistemas de la institución en los cuales pueden manipular y consultar información, para ello podemos implementar:

1. Establecer una lista de autorizadores a los cuales les llegue la solicitud del usuario que está solicitando el acceso al sistema.
2. El usuario deberá proporcionar justificación para el acceso, que será documentado como soporte.
3. Una vez otorgado el acceso, se le deberá asignar al usuario un ID único, siendo este el identificador del empleado.
4. Concientizar al empleado que el ID y contraseña no deben de ser compartidos, ni prestados.

Como parte de las funciones del área de control interno se encuentra la implementación de un documento en el cual se enlisten cada una de las facultades que tiene el empleado, las funciones que realiza, el tipo de información que maneja (pública, privada, confidencial, restringida, etc.) cuyo objetivo es compartir los registros con el supervisor del empleado para su respectiva revisión, él será el responsable de verificar que los accesos que tiene el empleado sean de acuerdo a las funciones que realiza, indicando al área de control si deben de eliminarse facultades si es que existió cambio de funciones o en su defecto si deben de agregarse a la lista de registros nuevas actividades del empleado, es importante mencionar que ningún empleado ya sea supervisor o gerente, podrá auto gestionar la eliminación de facultades. Este documento es de gran ayuda a la institución ya que es una manera de tener un control más robusto al contar con el detalle de cada uno de los empleados que forman parte de ella.

Otro punto de control que debe ser considerado, es cuando se efectúa el cambio de área, deberán de ser eliminados aquellos accesos que ya no formen parte de las nuevas funciones del empleado, cuya finalidad será prevenir el uso inadecuado de la información, el riesgo a algún fraude interno o estar coludido con alguien externo, de esta manera, se está protegiendo la información del área y de la institución; esta práctica también deberá ser utilizada para los empleados que renuncian a la institución, para ello se deberá de realizar:

1. El retiro de la credencial de acceso a la institución.
2. Eliminación de facultades a los sistemas de la institución.
3. Eliminación de su ID único.
4. Respaldo de información que se encuentra en su equipo de cómputo.
5. Notificación al equipo de seguridad, con la finalidad de que no permitan el acceso a los edificios, de ser necesario deberá de contar con una autorización.
6. Verificación de que el empleado no retire información (USB, carpetas, etc.) perteneciente a la institución.

De esta manera evitaremos que el ex empleado pueda realizar algún fraude, o de a conocer información importante de la institución.

2.3.2.1 Administración de acceso con derechos privilegiados.

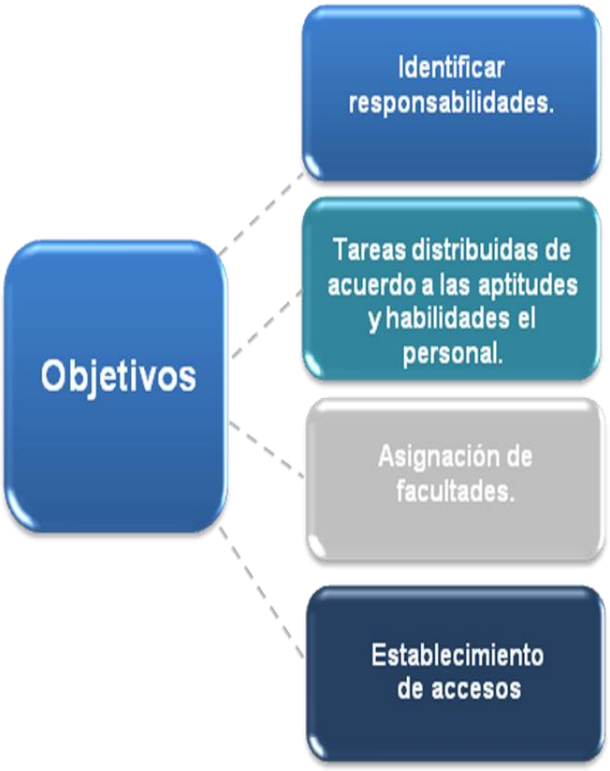
Los accesos privilegiados es una manera más específica de mantener controlado la consulta o manipulación de la información, ya que ello dependerá de la función que realiza el empleado, para que se le sean otorgadas las facultades acordes a sus actividades diarias y así obtener acceso a la información. Al minimizar los privilegios nos aseguramos el acceso de información a la persona correcta.

En esta parte del control veremos la importancia de creación de perfiles.

Perfiles. Es el conjunto de derechos concedidos y denegados a un usuario dependiendo de su rol en la organización se denomina perfil de acceso o simplemente perfil.[11]

La importancia de la creación de perfiles es que nos ayudará a generar e identificar los roles y/o actividades que realiza el empleado, permitiéndonos definir los permisos a los cuales tendrá derecho para tener acceso a la información.

[11] Aceituno Canal Vicente / Seguridad de la Información / Creaciones Copyright.



La asignación de facultades estará bajo la responsabilidad del dueño de la información o también conocido como “Supervisor” del departamento; en conjunto con el área de control deberán crear un documento oficial en el que se detalle lo siguiente:

1. Área.
2. Nombre del empleado.
3. Funciones.
4. Responsabilidades.
5. Tipo de información que maneja.
6. Formato en el cual se encuentra resguardada la información (papel, computadora asignada, en un sitio de red compartido del área, etc.)
7. Facultades y accesos que tendrá.
8. Firmas del empleado, supervisor y área de control.

Como lo hemos visto anteriormente en un departamento integrado por diversas personas existe la segregación de funciones, es decir cada uno de ellos tiene actividades específicas que realizar, por lo cual solo será encargado de manipular o consultar información que esté relacionada con sus funciones, por ejemplo, se puede llevar a cabo la creación de un sitio compartido, en el cual se pueden otorgar facultades especificas de acuerdo a la función de la persona como a continuación se muestra:

Sitio compartido del departamento staff:

Función:

Consulta información y/o registros.

Facultades

1. Vista de información.

Función:

Carga de información y mantenimiento del sitio.

Facultades

1. Vista de información.
2. Descarga de información.
3. Modificar información.

Facultades

1. Vista de información.
2. Descarga de información.
3. Modificar información.
4. Eliminar información
5. Control de accesos.
6. Acceso al historial.

Función:

Elaboración de métricas.

Función:

Supervisor del proceso.

2.3.2.2 Administración de password.

En la actualidad la mayor parte de la información se encuentra en equipos informáticos, soportes de almacenamientos y redes de datos, ellos están más propensos a amenazas que pueden generarse desde dentro de la institución o ser atacados por personal externo.

Uno de los pasos más importantes para salvaguardar información es proteger la información por medio de contraseñas, ya que ella funciona como un candado o una cerradura que nos ayudará a tener resguardada y protegida nuestra información de cualquier persona ajena.

Una contraseña es la combinación de caracteres que pueden ser alfa numéricos o solo numéricos, la cual debe ser creada por el dueño del equipo de cómputo para poder tener acceso a este, también deberá crear una contraseña para el ingreso a sistemas pertenecientes a la institución y que previamente se le haya otorgado la facultad de acuerdo a sus funciones.

Al crear una contraseña se debe de pensar en el grado de seguridad que se quiere implementar a la información, es decir, si los datos son clasificados como confidenciales o restringidos, se requiere de una contraseña más compleja que nos proporcione mayor seguridad.

CONSEJOS PARA CREAR UNA CONTRASEÑA SEGURA:

1. No utilizar datos personales como:
    a) Nombre.
    b) Fecha de nacimiento.
    c) Número de teléfono.
    d) Dirección.
    e) Nombre de padres, hijos, esposa, novia, etc.
2. Utilizar letras y números.
3. Alternar mayúsculas y minúsculas
4. Fácil de recordar.

El empleado debe de estar consciente que tener una contraseña, es un método de control que le permitirá proteger la información que utiliza, debiendo tener ciertos controles y cuidados para su manejo, por ejemplo:

1. No debe de ser compartida.
2. Debe procurar que nadie vea su contraseña al digitalizarla.
3. Su contraseña deberá tener vigencia, con la finalidad que deberá ser cambiada con cierta periodicidad.
4. Los sistemas deberán de estar configurados para que la contraseña no sea visible en la pantalla del monitor.
5. Deberá de ser memorizada, evitando escribirla en un papel ya que pone en riesgo que alguien pueda hurtarla o copiarla.
6. Los sistemas deberán de estar configurados en bloquear o inhabilitar el acceso al sistema después de 3 intentos fallidos al ingresarla.
7. No deberá de ser guardada en el sistema.

Cada medida de control debe de ser operada correctamente para el cumplimiento de nuestras expectativas, de esta manera podemos evitar el acceso a una persona ajena.

2.3.3 Seguridad física.

Aunque la mayoría de riegos se da de manera digital, también debemos de considerar aquellos riesgos físicos que pueden perjudicar la disponibilidad y seguridad de nuestra información y recursos de la institución y/o clientes, en la actualidad debido a los avances tecnológicos y el riesgo que ello implica se presta mayor atención a las medidas de seguridad y control para proteger la información, dándole la menor importancia a los aspectos físicos que también implican un riesgo.

Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. [12]

Es decir, la seguridad física serán aquellas medidas de control y mecanismos a utilizar para resguardar la información de incidentes físicos que pueden ser ocasionados incidentalmente por el hombre o por la naturaleza.

[12] Villalón Huerta, Antonio / Seguridad en Unix y Redes.

Podemos considerar como riesgo físico aquellos accidentes por causas naturales, o también por uso, y continuo contacto con los documentos; es decir pensemos en aquella información que se encuentra en papel, puede existir el desgaste de documentos por determinado tiempo desde su creación, es por ello la importancia de resguardar la información en archiveros, siempre recordando el control y protección contra personal ajeno, por lo cual el archivero deberá de contar con llave, la cual solo el dueño de la información y/o proceso será el encargado de portarla.

Otros riesgos en los cuales también nuestra información puede verse perjudicada son por aquellas catástrofes naturales, los cuales no podemos controlar, pero si podemos implementar acciones y herramientas que nos ayuden a resguardar y proteger la información de la institución y de los clientes; dichos desastres pueden ser:

Durante un terremoto o temblor es muy complicado y riesgoso guardar o proteger la información, debido que lo primordial que se debe proteger es la seguridad de los empleados, sin embargo, para evitar incidentes es necesario que la institución implemente medidas de seguridad, por ejemplo:

1. No situar equipos en sitios altos para evitar caídas.
2. No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos.
3. Separar los equipos de las ventanas para evitar que materiales caigan por ellas.
4. Utilizar fijaciones para elementos críticos.
5. Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.
6. Proporcionar capacitaciones y materiales a los empleados, de las medidas de seguridad que deberán de implementarse.
7. Archiveros reforzados, construidos con material resisten que soporta gran peso, evitando la destrucción de nuestros documentos en papel.

Un incendio puede ser causado por fallas eléctricas ya sea por instalaciones defectuosas o el mal uso de los empleados en instrumentos electrónicos, poniendo en riesgo la vida de nuestros empleados y los activos de la empresa, algunas de las medidas de control que podemos implementar para la protección de información son:

1. Archiveros anti fuego, los cuales están diseñados para soportar altas temperaturas.
2. Extintores manuales.
3. Instalación de extintores y/o rociadores en el techo.
4. Instalación de sistema o bomba de agua, para la respectiva conexión de los bomberos.
5. Prohibir a los empleados el uso de sustancias y/o materiales inflamables como, velas, cerillos, spray, y fumar dentro de las instalaciones.
6. Proporcionar capacitaciones y materiales a los empleados, de las medidas de seguridad que deberán de implementarse.

Una inundación puede ser provocada por tormentas, o por algún descuido del personal, para lo cual podemos considerar las siguientes medidas:

1. Evitar colocar el archivo en sótanos, ya que son los primeros niveles que se ven invadidos de agua.
2. La utilización de archiveros anti fuegos también ayudan contra este fenómeno, debido a que está diseñado para no permitir la introducción de agentes ajenos.
3. Toda instalación eléctrica debe de estar resguardada, es decir no deberá de existir ningún cableado fuera de tubos PVC o como lo conoce coloquialmente, cable pelado.

La presentación de manifestaciones o huelgas, también pueden poner en riesgo nuestra información, debido a que se puede salir de control, llegando a realizar actos de vandalismo contra el edificio y el personal en su interior, por lo cual la institución deberá contemplar:

1. Equipo de seguridad privada, capacitado.
2. Instalación de cortinas de aluminio reforzado, las cuales permitan el cierre absoluto de la institución impidiendo el ingreso de manifestantes.
3. Circuito cerrado, instalaciones de sistemas de grabación alrededor de la institución, que permitirá observar el comportamiento de los manifestantes en el exterior y la culminación de la misma.
4. Los vidrios instalados en el edificio deberán de contener películas anti asalto, las cuales impedirán el rompimiento de las mismas, si los manifestantes arrojan materiales.
5. Instalación de alarma de seguridad, la cual al momento de su activación tenga comunicación con el equipo policiaco o bomberos de la zona.

Sin importar que incidente físico se presente, es importante implementar copias de seguridad de toda la información, es decir aquellos documentos que sean creados por medio de papel, los dueños del proceso deberán de generar una copia de respaldo de manera digital, es decir cada documento deberá de ser escaneado y grabado en un equipo de cómputo de la institución, USB o instrumentos que estén aprobados por la política de la institución.

Aquella información que se encuentra de manera digitalizado deberá de encontrarse en un sitio alterno o conocido también como nube creada en la institución. La información deberá de encontrarse cifrada, en caso de que los manifestantes lleguen a ingresar a la institución no puedan obtener acceso a ella.

2.3.4 Seguridad de la información con los proveedores.

Cuando compartimos información con terceros o personas externas a la institución debemos de establecer ciertos protocolos en la relación y en su defecto elaborar un contrato que nos permita establecer las responsabilidades, obligaciones, términos y clausulas en los cuales se llevará a cabo la comunicación y el trato que deberá de darse a la información que la institución le proporcione, dicho contrato debe ser de común acuerdo, esto con la finalidad de proteger los recursos de las personas involucradas.

Debido a que es prácticamente imposible asegurarnos el tipo de controles que maneja nuestro proveedor se podrá aplicar el control compensatorio, solicitando que la institución bancaria reciba un reporte semanal, mensual, trimestral o anual de acuerdo con las necesidades de la institución, esto con la finalidad de garantizar que la información proporcionada se encuentra debidamente resguardada.

A continuación, se enlistan ejemplos de servicios en los cuales la institución pudiera tener relación con proveedores:

1. Outsourcing.
2. Arrendamiento inmobiliario.
3. Seguridad Privada.
4. Equipo de marketing o publicidad.
5. Limpieza.
6. Proveedor de suministros de oficina (papelería).
7. Proveedor de suministros de cafetería.

Para tener relación con un proveedor la institución deberá de realizar un proceso de selección:

1. Planificación: es la fase en la cual la institución documenta sus requerimientos para un producto o servicio que debe ser proporcionado por un tercero, evalúa los riesgos inherentes asociados con la actividad y planifica cómo se manejarán los riesgos.
2. Selección de proveedor: Es la fase en la que se realiza las debidas evaluaciones de los diversos proveedores participantes, y las medidas de control requeridos, con el fin de seleccionar un tercero.
3. Contratación: es la fase en que se desarrolla, negocia y extiende el contrato que establece las expectativas, los derechos y las obligaciones de los terceros, incluyendo condiciones apropiadas de pago y gestión del riesgo.
4. Supervisión continua: es la fase en que se lleva a cabo la realización periódica de las evaluaciones de control aplicables, y las actividades de supervisión requeridas por el riesgo.
5. La terminación: es la fase de conclusión del servicio proporcionado por el proveedor, este puede ser derivado por incumplimiento de alguna de las dos partes o por finalización del contrato.

2.3.4.1 Monitoreo y supervisión de los proveedores.

La generación de una política para la administración de proveedores tiene la función principal garantizar que todas las actividades con terceros se realizan de forma correcta y segura en cumplimiento con las leyes, normas, reglamentos, políticas y normas de conducta. Esto impulsará que las prácticas de gestión sean acordes con el nivel de riesgo y complejidad de todas las relaciones con terceras partes (internas y externas)

Por ejemplo las agencias que son contratadas para los equipos de limpieza en una oficina, regularmente tienen acceso a todas las áreas de la institución en el cual pueden observar información ubicada en los escritorios del personal, lo conveniente como medida de control seria realizar un acuerdo de confidencialidad el cual deberá de contener aquellas acciones y consecuencias que pueden recurrir al infringir en algún lineamiento estipulado, este acuerdo deberá de estar firmado por los representantes legales de cada institución. Por ello la importancia de tener un convenio o contrato con cada uno de los proveedores, estipulando que se deberá llevar a cabo evaluaciones periódicas al proveedor con la finalidad de asegurarse del cumplimiento correcto y mitigación del riesgo.

Elementos a considerar para evaluar y/o escalar algún inconveniente con los proveedores:

1. Cumplimiento de políticas y contrato previamente firmado.
2. Incumplimiento del servicio, en tiempo y forma.
3. El personal que proporciona el servicio, deberá cumplir con los conocimientos esenciales para dar soporte.

Para llevar a cabo la evaluación de proveedor deberá de estar involucrada el área que está recibiendo el servicio, el área de control, y los representantes legales del proveedor, realizando un documento formal en el cual se enlisten:

1. Cumplimiento o incumplimiento del proveedor.
2. Los riesgos que hayan resultado de dicha evaluación.
3. Descripción del servicio proporcionado.
4. Medidas de corrección y prevención.

Si la evaluación al proveedor es negativa y riesgosa hacia la institución deberá de estipularse por medio del documento especificando el motivo por el cual se da el término de contrato.

2.3.5 Administración de incidentes de seguridad de la información.

Algunos controles compensatorios que debemos tomar en cuenta son:

1. En el lugar de trabajo: en ocasiones podemos no tomar atención aquella información impresa que tenemos en nuestros escritorios existiendo riesgo que ingrese alguien externo a la institución y pueda observar la información, facilitando su difusión. Por ello es conveniente considerar las siguientes medidas:

a) Guardar los materiales impresos que contengan información confidencial bajo un cajón o gabinete con llave.

b) Recopilar la información que se envió a imprimir en el momento, evitando que alguien ajeno tenga acceso a ella.

c) Cuando se realice una reunión en una sala de juntas o espacio compartido, borre aquella información analizada, recoja los folletos, carpetas que contenga información confidencial.

2. Eliminación de información: se deberá analizar la información impresa y digital, una vez que se haya cumplido con su objetivo y el tiempo de almacenamiento, se deberá desechar aquella información mediante alguna herramienta aprobada por la institución (trituradoras de papel, eliminación de base de datos en equipo de cómputo) con el objetivo de eliminar permanentemente aquellos datos que pongan en riesgo a la institución y sus clientes.

3. Descarga de programas o aplicaciones: existen softwares maliciosos diseñados para perjudicar los equipos de cómputo, por los cuales se puede accesar a información confidencial cargada en el equipo, poniendo en riesgo contactos de clientes, informes financieros, contactos comerciales, etc. Por ello es de suma importancia dar a conocer a los empleados de la institución que la descarga de softwares o el ingreso de sitios de internet ajenos pueden ser perjudiciales, de esta manera el empleado crea conciencia del riesgo que puede surgir.

Los controles compensatorios que se pueden aplicar son:

1. El área de sistemas deberá mantener actualizado el antivirus más reciente.
2. Limitar el acceso a páginas de internet ajenas de la institución.
3. Manejar solo facultades para acceso de correo interno.
4. Las sesiones que no se encuentren activas durante cierto lapso de tiempo, el equipo de cómputo deberá de bloquearse automáticamente.

Capítulo 3 Prevención de lavado de dinero en las áreas operativas de una institución bancaria.

3.1 Definición y su importancia.

En el mercado mundial, el intento de utilizar instituciones financieras es muy común para llevar a cabo operaciones relacionadas con el “Lavado de Dinero y el financiamiento al Terrorismo”, es por ello la importancia y concientización para crear controles y estándares mínimos que fortalezcan a la institución de mitigar este tipo de riesgo.

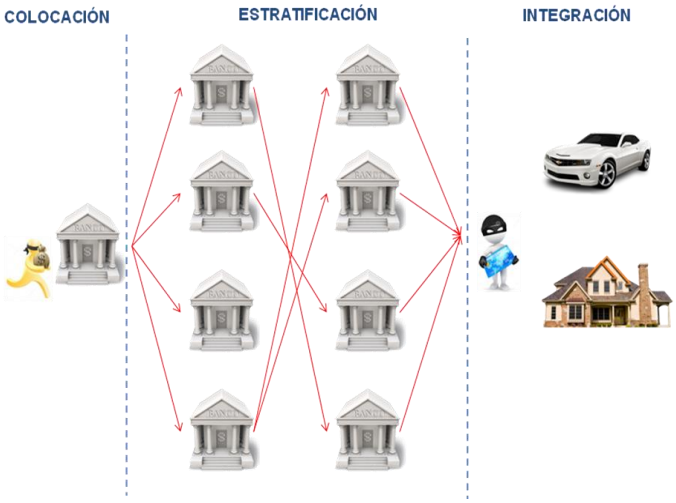
El “Lavado de Dinero” es considerado como aquellas operaciones efectuadas con recursos de procedencia ilícita, es decir, es el acto de adquirir, enajenar, administrar, custodiar, invertir o transferir, pudiendo ser dentro del territorio nacional, de éste hacia el extranjero o a la inversa, recursos, derechos o bienes de cualquier naturaleza, con conocimiento de que proceden o representan el producto de una actividad ilícita, con alguno de los siguientes propósitos: ocultar, encubrir o impedir conocer el origen, localización, destino o propiedad de dichos recursos, o alentar alguna actividad ilícita.[13]

[13] Art. 400 Bis del Código Penal Federal.

De acuerdo a la CNBV el lavado de dinero es el proceso a través del cual es encubierto el origen de los fondos generados mediante el ejercicio de algunas actividades ilegales (siendo las más comunes, tráfico de drogas o estupefacientes, contrabando de armas, corrupción, fraude, trata de personas, prostitución, extorsión, piratería, evasión fiscal y terrorismo).

Podemos considerar como actividades ilícitas los siguientes ejemplos:

ETAPAS DEL LAVADO DE DINERO



Colocación: es la acción en la cual se introduce el dinero obtenido por aquellas actividades ilícitas al sistema financiero.

Estratificación: es el movimiento del dinero dentro del sistema financiero, simulando transacciones complejas con el objetivo de ocultar el origen del recurso, es decir se realizan diversas transacciones para dificultar el rastreo.

Integración: es la última etapa en la cual el dinero es integrado a la economía para que comience a circular y aparente ser de una manera legítima.

REGULACIONES PARA PREVENCIÓN DE LAVADO DE DINERO.

El Grupo de Acción Financiero o también conocido como GAFI es un organismo internacional que se encargó de emitir 40 recomendaciones para la prevención de "Lavado de Dinero y combate al Financiamiento del Terrorismo"; estas recomendaciones se convirtieron en un proyecto mundial de controles efectivos para combatir el lavado de dinero nacional e internacional, contienen los estándares mínimos que deben observar los países y jurisdicciones miembros de este organismo con la finalidad de combatir el lavado de dinero.

Las recomendaciones más destacadas son:[14]

1. Evaluación de riesgos y aplicación de un enfoque basado en riesgo: esta recomendación está enfocada a que los países deben de realizar un análisis e identificación de sus riesgos en el tema de PLD con la finalidad que tomen las medidas necesarias para prevenir o mitigar este tipo de riesgo.
2. Cooperación y coordinación Nacional: cada país debe de establecer políticas a nivel nacional y designar una autoridad que se haga responsable de la implementación y revisión continúa de las políticas.
3. Sanciones financieras relacionadas al terrorismo y al financiamiento del terrorismo: hace mención al establecimiento de sanciones financieras, que deberán de cumplir aquellas organizaciones o personas que participen de manera directa o indirecta en dichas actividades, por ejemplo, la congelación de fondo.
4. Debida diligencia del cliente: las instituciones financieras deberán contar con toda la información del cliente, con la finalidad de que tengan la seguridad de a quién se le está proporcionando el servicio.
5. Mantenimiento de registros: las instituciones financieras deben de resguardar la información de todas las transacciones realizadas de manera nacional e internacional por al menos 5 años, debido a que dicha información puede ser utilizada como evidencia en algún juicio, la cual deberá de contener los montos, la moneda y las cuentas relacionadas.
6. Transferencias electrónicas: para este tipo de operaciones las instituciones financieras deben de tener el conocimiento de la persona que origina la operación y el beneficiario; implementando el monitoreo de dichas transacciones con la finalidad de detectar aquellas que carezcan de información o sea de manera inusual, teniendo la autoridad para congelar dichas operaciones.

[14] Grupo de Acción Financiero Internacional sobre el Blanqueo de Capitales.

7. Controles internos, filiales y subsidiarios: todas las instituciones financieras deben de contar con programas, capacitaciones, procedimientos, etc. Contra el lavado de dinero y financiamiento al terrorismo, dicho material debe de ser proporcionado a todos los niveles existentes dentro de la institución.

8. Países de mayor riesgo: las instituciones deben de aplicar medidas de control intensificado hacia las relaciones comerciales y transacciones con personas físicas y morales, e instituciones financieras, procedentes de países para los cuales el GAFI tiene clasificadas como de alto riesgo.

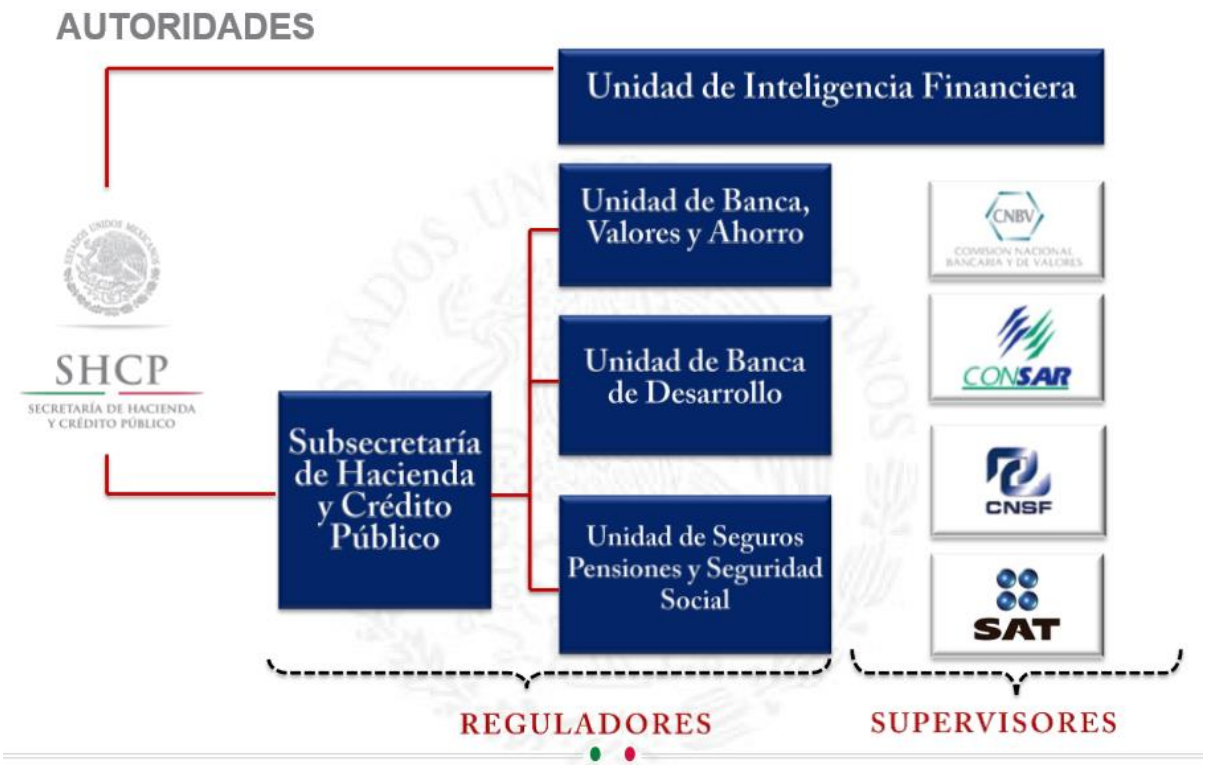
9. Reporte de operaciones sospechosas: toda institución financiera que cuente con motivos sustentables para sospechar respecto a los fondos obtenidos por alguna actividad criminal, deberá de enviar un reporte a la brevedad posible a la Unidad de Inteligencia Financiera (UIF)

10. Facultades de los supervisores: los países deberán de nombrar supervisores que cuenten con las facultades necesarias para llevar a cabo el monitoreo y supervisión a las instituciones financieras con la finalidad de asegurar el cumplimiento de las políticas y recomendaciones para combatir el lavado de dinero y financiamiento al terrorismo; los supervisores también deberán de contar con facultades para emitir sanciones disciplinarias, financieras, restringir o suspender la licencia de la institución, en caso de incumplimiento.

11. Unidades de inteligencia financiera: cada país debe de establecer su “Unidad de Inteligencia Financiera” quien estará encargada de recibir los reportes de sospecha emitidos por las instituciones financieras, con la finalidad de llevar a cabo el análisis de la actividad sospechosa, la entidad deberá de contar con la facultad de tener acceso a toda información financiera, administrativa y de orden público de las personas involucradas en la actividad ilícita.

LEY DE INSTITUCIONES DE CRÉDITO (Regulación Local).

A continuación, se mostrará los reguladores locales.



Fuente: Comisión Nacional Bancaria y Valores.

Secretaría de Hacienda y Crédito Público: tiene como misión proponer, dirigir y controlar la política económica del Gobierno Federal en materia financiera, fiscal, de gasto, de ingresos y deuda pública, así mismo supervisar a la CNBV la CNSF, Banxico, CONDUCEF y CONSAR.

Unidad de Inteligencia Financiera: de acuerdo a la recomendación 29 de la GAFI cada país deberá contar con esta unidad cuya finalidad es recibir y analizar todos aquellos reportes en materia de lavado de dinero a nivel nacional, buscando prevenir y combatir el lavado de dinero mediante el establecimiento de políticas y procedimientos.

Subsecretaría de Hacienda y Crédito Público: se encarga de supervisar la Unidad de Banca Valores y Ahorro, Unidad de Banca de Desarrollo y la Unidad de Seguros Pensiones y Seguridad Social; a su vez depende la SCHP, dentro de sus principales funciones está el presentar los proyectos y convenios internacionales correspondientes de las unidades mencionadas anteriormente, debido a la dependencia que tiene con la SCHP comparten el mismo objetivo, el cual es proponer, dirigir y controlar la política económica del Gobierno Federal.

REGULADORES.

Unidad de Banca, Valores y Ahorro: es la autoridad reguladora de las instituciones que contemplen actividades financieras como; bancaria, crediticia y de valores, se encarga de interpretar las leyes o disposiciones financieras que serán sujetas a aquellas instituciones que se encuentre bajo su regulación.

Unidad de Banca de Desarrollo: es la encargada de coordinar las instituciones de banca de desarrollo, las cuales son entidades de la "Administración Pública Federal" teniendo su patrimonio propio y personalidad jurídica al formar parte del sistema bancario mexicano dentro de sus principales funciones es el proporcionar financiamiento a personas físicas y morales, esta banca se ha convertido en una herramienta fundamental para promover el desarrollo buscando mejorar las condiciones para el crecimiento económico y empleo, enfocándose en el sector de MIPYMES (micro, pequeñas y medianas empresas), así como también en la infraestructura pública y financiamiento a los productores rurales.

Unidad de Seguros, Pensiones y Seguridad Social: es la encargada del establecimiento de políticas y la resolución de asuntos relacionados a instituciones encargadas de seguros, fianzas, fondos para el retiro, etc., dichas instituciones deben de estar sujetas a la vigilancia e inspección de la Comisión Nacional de Seguros y Fianzas o de la Comisión Nacional del Sistema de Ahorro para el Retiro.

SUPERVISORES.

Comisión Nacional Bancaria y de Valores o conocida por sus siglas como la CNBV es un órgano descentralizado o independiente de la SHCP, es la encargada de la regulación, supervisión y establecimiento de sanciones a aquellas instituciones financieras tales como bancos, auxiliares de crédito, casas de bolsa, y organismos bursátiles que se encuentran prestando servicios en México.

Comisión Nacional del Sistema de Ahorro para el Retiro o también conocida por sus siglas como CONSAR también es un órgano independiente a la SCHP, encargado de regular el "Sistema de Ahorro para el Retiro" quien administra las AFORES de los trabajadores dados de alta.

Comisión Nacional de Seguros y Fianzas es la encargada de supervisar aquellas instituciones involucradas en el sector de seguros y fianzas.

Servicio de Administración SAT, es el encargado de recaudar los recursos tributarios y aduaneros de las personas físicas y morales.

De acuerdo al artículo 115 de la Ley de Instituciones de Crédito, establece las diversas obligaciones entre las cuales destacan:

1. Establecer medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones que pudieran favorecer actos ilícitos.
2. Presentar a la SHCP por conducto de la CNBV, reportes sobre cierto tipo de operaciones que realicen con sus clientes y usuarios, o bien, que realicen los miembros del consejo de administración, directivos, funcionarios, empleados y apoderados bajo ciertos supuestos.
3. Observar los procedimientos y criterios que emita la SHCP en materia de identificación y conocimiento del cliente e identificación de usuarios.
4. Resguardar y garantizar la seguridad de la información y documentación relativas a la identificación de clientes y usuarios, así como de las operaciones y servicios que hayan sido reportados a las autoridades.

Cabe mencionar que dicho artículo también puede destacar ciertas sanciones en caso de incumplimiento, por ejemplo:

1. Las violaciones a las disposiciones establecidas serán sancionadas por la CNBV, con una multa equivalente del 10% al 100% de la operación inusual reportada y en los demás casos en una multa equivalente de 30,000 a 100,000 días de salario.[15]

Como hemos observado en este primer punto del capítulo, es importante que toda institución cree conciencia respecto al mercado globalizado, la inteligencia y malicia que los grupos organizados han ido desarrollando con el transcurso de los años. Una adecuada dirección y comunicación en todos los niveles, es decir desde los altos Directivos hacia los demás empleados es de vital importancia, ya que ellos al estar involucrados y ser dueños de sus procesos pueden identificar aquellas operaciones inusuales que pongan en riesgo a la institución.

Tal y como vimos la primera herramienta que nos ayudará a combatir el lavado de dinero y/o financiamiento al terrorismo, es conocer a nuestro cliente, es decir tener la mayor información al respecto de él, sus actividades, el giro comercial con quien tiene relación en ese ámbito, etc. Pero también podemos robustecer nuestro control creando una estructura que nos ayude a identificar los riesgos desde distintos niveles conocido como:

[15] Comisión Nacional Bancaria y de Valores.

TRES LÍNEAS DE DEFENSA.

1. La primera línea de defensa son las “Unidades de negocio y/o áreas operativas”, son las áreas que tienen el primer contacto con los clientes y ejecutan las operaciones solicitadas, por esta razón son asignados como “La Primera Línea de Defensa” ya que son los primeros en poder identificar y evaluar los riesgos que puede presentar una actividad solicitada por el cliente, esta primera línea es responsable de la administración de toda la información relacionada con el cliente; sus principales funciones son:

    a) Identificar y reportar a la segunda línea de defensa los riesgos operativos en el momento en el que surjan.

    b) Debe contribuir y ejecutar los controles clave previamente estipuladas por la Dirección de Control Interno.

    c) Cumplir con las políticas previamente establecidas.

    d) Mantener el expediente y/o información de cliente actualizada y correctamente resguardada.

2. Segunda línea de defensa es el área de “Compliance o Control interno” encargada de PLD, su principal objetivo es mejorar la efectividad de los controles a través de una relación muy cercana con el área de negocio, debiendo trabajar conjuntamente para crear una cultura en la administración del riesgo operacional para combatir el lavado de dinero; sus principales funciones son:

    a) Establecimiento de controles.

    b) Seguimiento del cumplimiento de las políticas relacionadas a la prevención del lavado de dinero.

    c) Proporcionar soporte para la primera línea en casos de sospechas.

    d) Coordinarse con el área de cumplimiento institucional y jurídico para determinar los procesos para atención de los requerimientos regulatorios.

    e) Notificar a la CNBV el informe de auditoría interna para evaluar el cumplimiento de las disposiciones de PLD.

    f) Evaluar el impacto de las nuevas regulaciones y políticas en su negocio y colaborar en su implementación.

3. Tercera línea de defensa “Auditoría Interna”, su principal objetivo es evaluar los controles de manera periódica con apoyo del área de compliance; sus principales funciones son:

    a) Verificar el correcto cumplimiento de las políticas y procedimientos establecidos contra el lavado de dinero.

    b) Realizar evaluaciones y revisiones independientes.

    c) Entregar evaluaciones e informar la efectividad de los controles implementados.

    d) Monitoreo de las decisiones tomadas de acuerdo a las evaluaciones anteriores.

3.2 Conocimiento e identificación del cliente.

Con el fin de prevenir el lavado de dinero, los reguladores e instituciones financieras establecen mecanismos que permiten identificar a sus clientes con el fin de verificar el origen y destino de los recursos, a continuación, se describe los principales conceptos que ayudan en dicha identificación.

Cliente: es aquella persona física, moral o fideicomiso que directamente o por conducto de algún comisionista contratado por la institución realice las siguientes actividades:

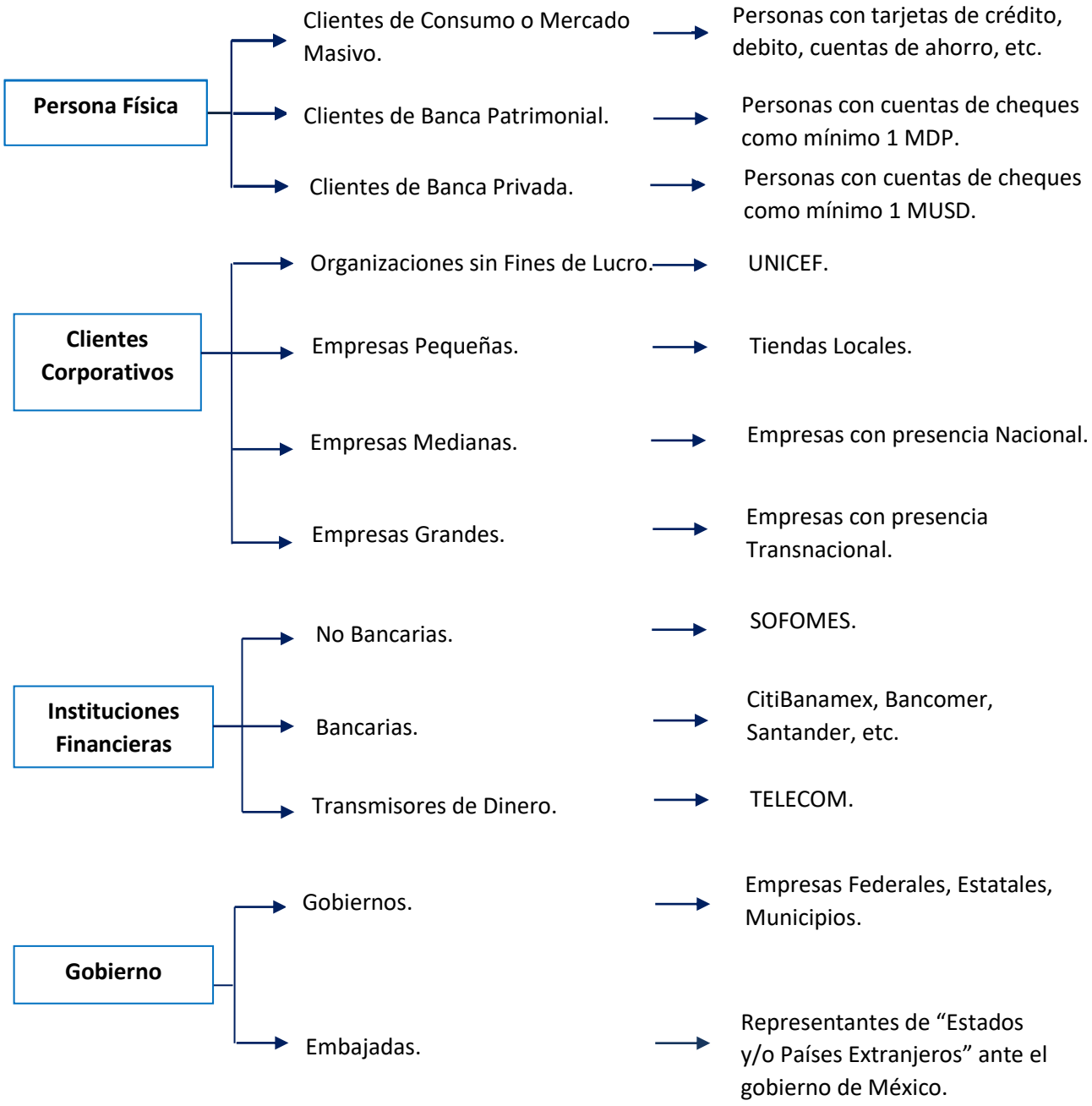
a) Actué a nombre propio o a través de mandatos o comisiones, que sea cuentahabiente de la institución.

b) Utilicé al amparo de un contrato, los servicios prestados por la institución o realicé operaciones con esta.

De acuerdo a la Unidad de Información Financiera (UIF) cliente es toda aquella persona física o jurídica con la que se establece, de manera ocasional o permanente, una relación contractual de carácter financiero económico o comercial.

Resumiendo, las definiciones anteriores podemos definir que un cliente es la persona ya sea física o moral, con la cual realizaremos una relación comercial formalizada por medio de contratos y/o acuerdos.

Clasificación de clientes en una Institución Bancaria.



Adicional a la clasificación anterior, también es importante considerar la siguiente:

Cliente de Alto Riesgo (CAR), en esta clasificación se pueden considerar personas físicas o morales que de conformidad con el marco regulatorio mexicano y políticas corporativas en materia de prevención de lavado de dinero sean considerados como un riesgo potencial hacia la institución. Principalmente se consideran de alto riesgo a aquellas empresas o personas físicas que manejan continuamente altas cantidades de dinero en efectivo como:

a) Casinos.

b) Bufetes de abogados.

c) Contadores.

d) Empresas de beneficencia.

Para cada uno de los clientes mencionados anteriormente es necesario solicitar información y cumplir con requerimientos específicos de identificación, con la finalidad de realizar análisis e identificar a los clientes de acuerdo al nivel de riesgo que puede implicar hacia la institución, dicha determinación se puede basar por los siguientes factores:

a) Índole socio demográfico.

b) Transaccional.

c) Reputacional.

Es por ello la importancia de crear un perfil de cliente bajo la metodología de control llamada “Conoce a tu Cliente” o en sus siglas en ingles KYC (Know Your Customer), este modelo es de vital importancia para robustecer el control en la institución, su principal objetivo es evitar que los bancos se conviertan en blanco fácil de lavado de dinero que procede de actividades ilícitas como el terrorismo, narcotráfico, crimen organizado, etc. Este control lleva a cabo una identificación formal de los clientes mediantes ciertos procedimientos y políticas que debe cumplir la institución.

Importancia de conoce a tu cliente (KYC):

1. Protege la integridad de los sistemas bancarios.
2. Protege la reputación de la institución.
3. Protege la integridad de los clientes.
4. Evita que la institución sea utilizada como vehículo para el lavado de dinero.
5. Evita problemas legales y multas.

La institución financiera deberá de elaborar sus políticas y procedimientos que establezcan lo primordial para mantener una relación comercial con el cliente.

COMPONENTES DE CONOCE A TU CLIENTE (KYC)

El modelo conoce a tu cliente se basa en cinco componentes, cada uno de ellos tiene la finalidad de responder preguntas específicas y fundamentales que contribuirán en el estudio y conocimiento del cliente:

1. Identificación del cliente, este elemento se centra en determinar la identidad del cliente ya que se enfoca a responder la pregunta ¿Quién es el Cliente?, establece y valida su identidad mediante la solicitud y recolección de información que permita comprobar que el cliente es quien dice ser.

2. Lista de clasificación de clientes, está diseñada para identificar a personas físicas o morales que pueden ser un riesgo para la institución, este elemento responde a la pregunta ¿Podemos o debemos hacer negocio con este cliente? Es de vital importancia revisar la “Lista de sanciones” del Departamento del Tesoro de la Oficina de Control de Activos Extranjeros (OFAC) y “Lista de Personas Bloqueadas” emitida por la Secretaria de Hacienda y Crédito Público, en el momento que se está llevando a cabo la relación comercial entre el cliente y la institución financiera, de esta manera se podrá verificar la veracidad y seguridad de aperturar cuenta(s)al cliente.

3. Debida identificación del cliente, bajo este elemento se solicitan los requisitos mínimos de regulaciones mexicanas para identificación del cliente, es el proceso de obtener y revisar la información del cliente para evaluar los riesgos asociados con el cliente y sus actividades bancarias que pretende realizar, respondiendo a la pregunta ¿Podemos hacer negocios con el cliente y controlar adecuadamente los riesgos? Bajo este elemento se puede obtener la siguiente información:

    a) Geografía.

    b) Negocio y/o empleo.

    c) Finanzas.

    d) Propiedad beneficiosa, etc.

4. Debida identificación del cliente de alto riesgo, este proceso es requerido para aquellas personas o corporaciones que son consideradas por la movilidad de dinero en efectivo, es necesario realizar un análisis más detallado.

5. Perfil del producto, este elemento ayudará a documentar las actividades bancarias del cliente, es decir el tipo de producto y/o servicio que el cliente planea utilizar, este varía según el tipo de cliente y su calificación de riesgo, respondiendo la pregunta ¿Cómo planeamos servir a este cliente, esto es apropiado en base a lo que sabemos sobre el cliente? Ciertos tipos de cuentas, productos y servicios suponen un riesgo mayor para el lavado de dinero y requieren un perfil más detallado para documentar la actividad esperada, por ejemplo, las cuentas de transacción son cuentas a través de las cuales se pueden realizar o recibir transferencias, estos son particularmente vulnerables al lavado de dinero y al financiamiento del terrorismo.

Estos elementos en conjunto nos permiten formar una creencia razonable, de conocer la verdadera identidad de cada uno de los clientes, sus necesidades bancarias y los riesgos asociados con su servicio.

A continuación, se muestra un ejemplo de formato a utilizar para la identificación del cliente, cabe mencionar que este puede ser modificado de acuerdo a las actualizaciones solicitadas por los reguladores locales.

FORMATO DE EJEMPLO "CONOCE A TU CLIENTE (KYC)"[16]

Número de Folio: **Fecha**: - - **Promotor**:	
I. DATOS GENERALES	
Nombre: **Sexo: Masc**. ☐ **Fem**. ☐	
Fecha de Nacimiento: - - **RFC**: – **CURP**:	
Estado Civil: **Nacionalidad**: **e-mail**:	
Domicilio Particular: **Colonia**:	
Delegación o Municipio: **Estado**: **CP**:	
Teléfono Particular: - - **Teléfono Of**: - - **Ext.** **Cel**: **Fax**: - -	
II. INFORMACIÓN LABORAL DEL CLIENTE	
Empresa en la que labora:	**Antigüedad**: **a m**
Descripción de la operación del negocio:	
Posición: **Profesionista**: ☐ **Empleado**: ☐ **Inversionista**: ☐ **Directivo**: ☐ **Empresario**: ☐	
☐ **Mismo** **Domicilio Oficina**: **Colonia**:	
Delegación o Municipio: **Ciudad y Estado**: **CP**:	
Teléfonos: - - **Fax**: - - **e-mail**:	
III. INFORMACIÓN FINANCIERA	
Principal fuente de ingresos ☐ **Salario** ☐ **Honorarios** ☐ **Negocio Propio** ☐ **Patrimonio/Ahorro/Pensión** ☐ **Rentas**	
Ingreso Anual Aproximado: $ **Referenciado por**:	
IV. COMPORTAMIENTO TRANSACCIONAL	
Monto Aportación Inicial: $	**Otras Cuentas de Inversión**: **Moneda:**

[16] Fuente Columbus de México Asesores Financieros

Estimación de Aportaciones y Retiros Mensuales:

Tipo de Transacción	Número de transacciones estimadas por mes.			Monto de operaciones estimadas por mes. (miles)		
	0 - 3	4 – 6	+ de 6	0 a 500	500 a 1000	+ de 1000
Depósitos	☐	☐	☐	☐	☐	☐
Retiros	☐	☐	☐	☐	☐	☐

Cuentas de Cheques Registradas para Retiros:

Banco:	**Banco**:
Número de Cuenta:	**Número de Cuenta**:
Sucursal: **Plaza**:	**Sucursal**: **Plaza**:
CLABE:	**CLABE**:

V. ORIGEN DE LOS RECURSOS (Patrimonio)

Indique el origen de los recursos: ☐ Patrimonio /Ahorro ☐ Herencia ☐ Honorarios /Sueldo
☐ Otros ☐ Ventas del Negocio ☐ Ventas de Inmuebles

VI. PROCEDENCIA DE LOS FONDOS (Tipo de Depósito)

Indique la procedencia de los fondos:
☐ Cheque ☐ Efectivo ☐ Transferencia de fondos, **Procede de**:

VII. INVESTIGACIÓN ACERCA DEL CLIENTE

¿El cliente es Figura Pública? ☐ SI ☐ NO ☐ Partido Político ☐ Gobierno ☐ Legislador
¿Alguno de los beneficiarios, es una figura pública individual o relacionada? ☐ SI ☐ NO
¿Tiene conocimiento de que actualmente se encuentre en algún litigio? ☐ SI ☐ NO

VIII. OBJETIVOS Y PREFERENCIAS DE INVERSIÓN, GRADO DE CONOCIMIENTO Y TOLERANCIA AL RIESGO

Conocimiento y Experiencia Financiera: Grado de conocimiento que tiene de cada uno de ellos:

PRODUCTOS	SI	NO	Alto	Moderado	Bajo
Sociedades de Inversión de Deuda	☐	☐	☐	☐	☐
Sociedades de Inversión de R. Variable	☐	☐	☐	☐	☐
Sociedades de Inversión de Cobertura	☐	☐	☐	☐	☐
Instrumentos de Deuda (CP y LP)	☐	☐	☐	☐	☐
Acciones	☐	☐	☐	☐	☐
Derivados	☐	☐	☐	☐	☐
Instrumentos emitidos en el Extranjero	☐	☐	☐	☐	☐

¿Qué porcentaje de su portafolio le gustaría mantener en efectivo para cubrir gastos inesperados?

☐ 20% ☐ 15% ☐ 10% ☐ 5% ☐ Nada

¿Si está de acuerdo en que la diversificación disminuye los riesgos potenciales (políticos, monedas, etc.), qué porcentaje de su portafolio estaría dispuesto a invertir en acciones?

☐ + del 50% ☐ del 35% al 50% ☐ del 20% al 35% ☐ del 5% al 20% ☐ Nada

Marque todas aquellas clases de activos que estaría dispuesto a invertir en su portafolio:

☐ Inst. de duda CP (30d / 1a) ☐ Inst. de deuda LP (1a / + de 3a) ☐ Otras monedas (usd, Euro)

☐ Renta Variable Nacional ☐ Renta Variable Internacional ☐ Soc. de Inversión ☐ Coberturas

¿Cuál de las siguientes opciones describe mejor su Horizonte de inversión?

☐ Menos de 180 días ☐ de 180d a 1 año ☐ 1 – 3 años ☐ Más de 3 años

¿Con cuál de las siguientes opciones se identifica mejor en cuanto a la tolerancia al riesgo (volatilidad) de sus inversiones?

☐ Conservador: Acepta solo pérdidas muy pequeñas e infrecuentes en momentos difíciles de los mercados.

☐ Moderado: Acepta 3 - 6 meses de rendimientos negativos durante fases difíciles del mercado.

☐ Agresivo: Acepta rendimientos anuales negativos durante fases difíciles del mercado.

IX. REVISION Y APROBACIÓN
Con el fin de asegurar que el cliente es apropiado para el **Asesor Financiero**, es de vital importancia que toda la información requerida en este formato este completa, sea veraz y haya sido verificada por el Asesor Financiero. ***Confirmación del Asesor Financiero que refiere al cliente:*** Nombre: Puesto: Firma Asesor_____ Firma Aprobación _____ * *El presente documento quedará sin validez si presenta cualquier modificación, tachadura o enmendadura en cualquiera de las respuestas a las preguntas contenidas en el mismo.*

DOCUMENTOS A INTEGRAR EN EL EXPEDIENTE DE IDENTIFICACIÓN AL CLIENTE.

Al momento de abrir una cuenta o celebrar un contrato con el cliente se debe de considerar integrar y conservar un expediente durante toda la vigencia de la cuenta o contrato y posteriormente por un periodo no menor a 10 años.

Los datos que debe contener el expediente son:

<u>Para personas físicas:</u>

1. Nombre completo del cliente.
2. Género.
3. Fecha de nacimiento.
4. Lugar de nacimiento.
5. Nacionalidad.
6. Ocupación.
7. Domicilio particular.
8. Número de teléfono (s) en donde se pueda localizar.
9. Correo electrónico.
10. CURP.
11. RFC, etc.

Para personas morales:

1. Denominación o razón social.
2. Giro mercantil.
3. RFC.
4. Domicilio.
5. Fecha de constitución.
6. Nacionalidad.
7. Teléfonos.
8. Nombre(s) completo del “Administrador, Director, Gerente General, Apoderado y representante legal.

De manera adicional podrán utilizarse métodos no documentales auxiliares, los cuales consisten en aplicar métodos diferentes a la verificación de documentos físicos, por ejemplo:

1. Indagación: si el domicilio proporcionado por el cliente se encuentra fuera del área atendida por la institución, tendrá el derecho de preguntar al cliente la razón por la cual está abriendo la cuenta o celebrando el contrato fuera de su localidad.
2. Llamadas para confirmación de datos: consiste en realizar llamadas telefónicas al lugar de residencia de cliente para confirmar los datos relativos al domicilio, nombre, ocupación, etc.
3. Referencias bancarias: es la obtención de información respecto de cuentas que el cliente tenga en otra institución financiera.
4. Antecedentes crediticios (Consulta en el Buró de Crédito): cuando la institución lo considere necesario, debido a los productos o servicios que le proporcionará al cliente, la institución podrá solicitar la autorización del cliente para una consulta a sus antecedentes crediticios a través del “Buró de Crédito”.

Como toda medida de control KYC también requiere tener un seguimiento y/o actualización de la información que los clientes proporcionaron al momento de aperturar la cuenta, por ello es recomendable que la institución verifique cuando menos una vez al año que los expedientes de identificación de clientes cuenten con todos los datos y documentos previstos. Cada área o negocio deberá establecer sus procesos de verificación o actualización que resulten más convenientes de acuerdo al número y tipo de cliente con el cual fue clasificado, cuya finalidad es asegurarse que el cliente no realice operaciones inusuales o diferentes a lo que declaró al momento de celebrar el contrato con la institución financiera; este seguimiento y actualización de expediente nos ayudará a mantener la información más reciente de cliente, ya que no solo pueden existir cambios de información personal como dirección, teléfonos de contacto etc., también puede incrementar los productos y/o servicios que tiene con la institución, de ser así la institución deberá de realizar el análisis de riesgo sobre los nuevos productos

y el estudio económico del cliente debido a que debe existir un incremento de ingresos, de los cuales se debe de confirmar que no sean por medio de actividades ilícitas.

Podemos considerar como operación inusual aquella actividad, conducta o comportamiento de un cliente que no concuerde con los antecedentes o actividad conocida por la institución que fue declarada, o que exista un cambio en el perfil transaccional, es decir si el cliente solicita la apertura de una cuenta de nómina el banco deberá de establecer en el contrato la continuidad con la cual se recibirá transferencias de acuerdo a lo confirmado por el cliente, los depósitos pueden ser de manera semanal, quincenal o mensual; un foco de rojo que puede advertir a la institución financiera que el cliente está realizando una actividad inusual es que este percibiendo depósitos diarios, cantidades mayores de acuerdo a lo manejado en 3 o 6 meses, por lo cual la institución deberá de verificar con el cliente la procedencia de los recursos o la actividad actual que esté realizando, esto con la finalidad de prevenir el lavado de dinero.

3.3 Clientes de alto riesgo y no deseados para instituciones bancarias.

Es de suma importancia que las instituciones financieras, en su metodología de identificación del cliente o KYC como lo vimos en el capitulo anterior, el cual nos menciona la importancia de conocer a su cliente, su actividad comercial, el origen de sus ingresos, etc., puedan tomarlo como base para realizar la clasificación de sus clientes de acuerdo al nivel del riesgo que pueden implicar un peligro el tener una relación comercial, por ello nos enfocaremos en solo una clasificación mencionada en el tema 3.2 la cual es “Cliente de Alto Riesgo (CARs) debido a que este tipo de clientes pueden llegar a generar un gran impacto a la institución si no se realiza el análisis y control adecuado.

Se considera cliente alto riesgo[17] aquél que, por sus características como su nacionalidad, país de residencia, zonas geográficas de donde opera, así como el giro o actividad económica y perfil transaccional que tenga, puede facilitar la utilización o circulación de recursos que provengan de actividades ilícitas.

De acuerdo al artículo 115 de la “Ley de Instituciones de Crédito” se considerarán clientes de alto riesgo aquellos no residentes en el país y que se encuentren asignados al segmento conocido como banca privada, así como las personas políticamente expuestas, de igual forma, serán consideradas las personas morales que realicen operaciones en efectivo con dólares de los Estados Unidos de América.

[17] Morales Martha / Entrenamiento y Prevención del Crimen Financiero.

De acuerdo a las definiciones anteriores podemos resumir que los Clientes de Alto Riesgo o conocidos por sus abreviaturas como CARs, son aquellas personas extranjeras que fluctúan con monedas de otros países, personas pertenecientes al gobierno o que tengan relación alguna con él, y aquellas que de acuerdo al giro de su negocio son más propensas a participar en el lavado de dinero y poner en riesgo a la institución financiera.

*Personas Políticamente Expuesta o también conocida por sus siglas “PEP”, se refiere a aquella persona física nacional o extranjera que desempeña o desempeñó funciones públicas como; pertenecientes a algún partido político, militar o administrativo, altos ejecutivos de empresas estatales, embajadores, líderes sindicales, etc. La institución financiera también podrá considerar como cliente PEP al cónyuge, concubina, o todas aquellas personas que tengan parentesco con la persona que desempeño funciones públicas.

Una de las características fundamentales de los clientes mencionados anteriormente es debido a que manejan grandes cantidades de dinero en efectivo, el cual implica una dificultad para rastrear su origen, convirtiéndose en blancos fáciles para el lavado de dinero, en cuanto los PEPs debido a la actual corrupción existente en el país es prudente considerarlos en esta clasificación.

Además de los clientes mencionados anteriormente existe una característica más que puede hacer propenso a un cliente como alto riesgo y esto es debido a su nacionalidad o el país en donde se encuentra sus inversiones ya que algunos son considerados como alto riesgo. Existen países conocidos como “Paraísos Fiscales” debido a sus estrictas normas de secreto bancario que resguardan la información de los extranjeros inversionistas y que les permiten mover su dinero sin ningún tipo de fiscalización, se convierten en un blanco fácil para el lavado de dinero, algunos de estos países son:

1. Belice.
2. Barbados.
3. Bahamas.
4. Chipre.
5. Islas Caimán.
6. Islas Vírgenes.
7. Islas Bermudas.
8. Luxemburgo.

Existen variables específicas a considerar que nos ayudarán a analizar el riesgo que representa para la institución un CAR’s dichas variables son:

1. Tipo de cliente: persona física o moral.
2. Años de operar en el mercado.
3. Domicilio del cliente, en caso de persona moral validar la sucursal o corporativo en el que opera el cliente.
4. Nacionalidad.
5. País de origen.
6. Giro o actividad.

Una vez realizado el estudio de las variables mencionadas anteriormente para la obtención de nivel de riesgo que implica el cliente, es recomendable que la institución financiera valide continuamente la “Lista de Personas Bloqueadas” emitida por la Secretaria de Hacienda y Crédito Público, en ella se encuentran las personas y/o empresas que se realizan actividades ilícitas e impliquen un riesgo para la institución financiera y el sistema económico del país.

En caso de que la institución identifique al cliente en cuestión en la lista de personas bloqueadas deberá de:

1. Suspender inmediatamente la apertura de cuenta y/o contrato en cuestión.
2. Comunicar a las SCHP por medio del “Reporte de operaciones Inusuales” a la Comisión Nacional Bancaria y de Valores (CNBV) en un lapso de 24 hrs contadas a partir de la consulta en la lista de personas bloqueadas.

Es de suma importancia integrar a este tipo de clientes en la metodología de KYC mencionada en el punto anterior, es decir llevar a cabo la identificación del cliente, seguimiento y actualización de expediente, ya que la omisión de ello implica un riesgo mayor para la institución.

3.4 Procedimiento para clientes sujetos a revisiones adicionales.

Las revisiones y actualizaciones del expediente creado del cliente nos brindan la oportunidad de analizar la información y la actividad de cliente que fue establecida previamente. Con ayuda de estas revisiones puede ser actualizada la calificación de riesgo del cliente si es necesario, esto puede ser por incremento de productos, transaccionalidad más alta, cambio de giro comercial, etc.

Los clientes sujetos a estas revisiones son los CAR's (PEP's, Organizaciones no Lucrativas, abogados, contadores, etc.) ya que este tipo de clientes representan un mayor riesgo en materia de "Prevención de Lavado de Dinero", la revisión generalmente consta de los siguientes pasos:

1. Actualización de perfil: confirmar los datos del cliente (Nombre, domicilio, género, nacionalidad, etc.)
2. Revisión: realizar la consulta en la lista de personas bloqueadas emitida por la SHCP (regulación local) y la OFAC (regulación Internacional).
3. Revisión del perfil del producto: es recomendable considerar por lo menos 1 año del uso del producto como histórico para poder determinar si la actividad es razonable y proporcional al perfil del cliente, así como identificar y explicar las desviaciones observadas.
4. Revisión de la transacción a nivel de cuenta: es recomendable considerar 1 año del uso de la cuenta como histórico, con la finalidad de determinar si la actividad es razonable y proporcional al perfil del cliente, así como identificar y explicar las desviaciones observadas.
5. Informe de revisión: documentar los resultados de la revisión confirmando la coherencia con la información de KYC del cliente, mencionando las actualizaciones de haber sido necesario.

Para establecer una relación comercial con CARs es recomendable tomar medidas de control adicionales al momento de aperturar una cuenta o celebrar un contrato.

1. Aprobación por escrito o correo electrónico del director del área operativa o persona con facultades especificas para aprobar la apertura de la cuenta.
2. Aprobación por escrito o correo electrónico del director del área encargada a la prevención de lavado de dinero.
3. Verificación del domicilio del cliente, dejando alguna evidencia de la visita.
4. Aplicación de cuestionario de identificación de cliente.
5. Monitoreo e investigación continúo del comportamiento transaccional del cliente.
6. Tratándose de PEPs es recomendable dar seguimiento a la reputación del cliente a través de consulta de información pública disponible (Internet, periódicos, otras publicaciones).
7. En caso de que el cliente sea una embajada será necesario que indique el tiempo en que la embajada ha operado en territorio nacional y especificar si tiene varias oficinas con la dirección física de cada una de ellas.
8. El personal Directivo deberá reunirse periódicamente con la finalidad de analizar el estatus y situación de cada cliente considerado como “Cliente de Alto Riesgo”, con la finalidad de determinar el riesgo que implica y si es necesario tomar medidas de controles adicionales como parte de seguimiento.

En términos generales toda revisión deberá contar con evidencia de cada uno de los controles adicionales previamente mencionados, en caso de la ausencia de algún Vo.Bo de Dirección no podrá efectuarse la alta de la cuenta o celebración del contrato, con la finalidad de evitar cualquier riesgo implícito.

3.5 Reporte de operaciones a las autoridades.

Las instituciones financieras también tienen la obligación de realizar entrega de reportes relacionados a las operaciones del lavado de dinero por conducto de la CNBV y/o UIF.

Reporte de operaciones inusuales**:** consta en dar a conocer a las autoridades aquellas operaciones o el comportamiento transaccional del cliente que no concuerda con su histórico o con la actividad que le fue reportada a la institución, este tipo de comportamiento lo podemos observar en diferentes escenarios como:

a) Origen de los recursos.
b) Destino de los recursos.
c) El monto o cantidad transferida y la frecuencia con la que se realiza.

Para determinar que una actividad es inusual la institución financiera deberá de contemplar:

1. Antecedentes del cliente, así como su ocupación, profesión y giro de su negocio.
2. El monto y frecuencia de las operaciones que realiza.
3. Cuando el cliente se niegue a proporcionar los datos o documentos solicitados por la institución para su identificación.
4. Si el cliente intenta sobornar o intimidar a un empleado de la institución para que ejecute aquellas operaciones que están fuera de las disposiciones legales.
5. Cuando un cliente realiza transferencia a una persona que se encuentre en la lista de personas bloqueadas.

Reporte operación interna preocupante**:** se debe dar a conocer a las autoridades aquellas actividades provenientes de algún directivo, accionista, socio, y/o empleado, que se vieran involucrados en la participación de operaciones relacionadas con el lavado de dinero. Para identificar si un empleado está realizando actividades sospechosas o ilícitas, se deberá de analizar las siguientes características:

1. Si un empleado, directivo, representante o cualquier persona que forme parte de la institución muestra un nivel de vida superior al que le corresponde de acuerdo al nivel salarial que tiene asignado.
2. Si un empleado, directivo, representante o cualquier persona que forme parte de la institución haya participado en las operaciones que fueron reportadas como inusuales.
3. Si existe la sospecha que un empleado, directivo, representante o cualquier persona que forme parte de la institución haya omitido acciones de control o realizado alguna actividad que pudiera favorecer en la realización de operaciones provenientes del lavado de dinero.

Para evitar que los empleados se vean vinculados en este tipo de actividades es recomendable que las instituciones financieras realicen ciertas actividades y/o estudios que fortalezcan la relación empleado – institución.

1. Conoce a tu empleado: es recomendable que la institución realice diversos exámenes a los empleados al momento de la selección y reclutamiento, esto con la finalidad que se tenga el mayor conocimiento del empleado como; su conducta, valores, empleos anteriores, etc.
2. Análisis de inconsistencia: este tipo de análisis es de mayor factibilidad que el supervisor y/o compañeros cercanos al empleado lo pueden percatar, ya que consiste en detectar la diferencia entre el nivel salarial que percibe el empleado y el estilo de vida que tiene, otro factor importante es si existe discrepancia entre las funciones que le son asignadas y las que lleva a cabo.
3. Vinculación con operaciones inusuales: es de suma importancia analizar los reportes de operaciones inusuales que le son entregados a las autoridades, ya que en ellos se puede ver implicado la colaboración de un empleado, en base a ello se deberá investigar si fue una omisión por descuido o el empleado esta coludido con una persona vinculada en actividades ilícitas.

4. Motivación: es importante que la institución tenga una cultura en la cual se reconozca el esfuerzo de los empleados, sientan que forman parte de la institución, que son dueños de sus procesos, bien remunerado de acuerdo a sus funciones; un empleado que se siente feliz en donde trabaja, difícilmente pondría en riesgo su trabajo.
5. Capacitación: mantener continuamente informados a los empleados de las medidas de controles existentes en la institución, fomentar la concientización de los riesgos que existen y que pueden perjudicar no solo la institución si no también su trabajo.

Reporte de operación relevante: son aquellas operaciones mediante las cuales se realizan transferencias internacionales, aquellas operaciones por la cantidad de igual o mayor a $10,000 dólares americanos, esta puede ser en billete, moneda nacional, cheque de viajero o las monedas que son acuñadas de platino, oro o plata.

Tipo de Reporte	Breve descripción	Plazo de Entrega a las Autoridades
Operación Inusual	Aquellas actividades que no concuerdan con el comportamiento histórico del cliente.	Un periodo que no exceda de los 60 días naturales contados a partir de que se genere la alerta por medio del sistema, modelo, proceso o por el empleado, lo que ocurra primero.
Operación Interna Preocupante	Operaciones ilícitas en las cuales se encuentren vinculados personal que forme parte de la institución financiera.	Dentro de un periodo que no exceda los 60 días naturales contados a partir de que la entidad detecte la operación, por medio de su sistema, modelo, proceso o por cualquier empleado de la misma, lo que ocurra primero.
Operación Relevante	Operaciones efectuadas de un monto igual o mayor a $10,000 dólares.	10 primeros días hábiles de los meses de enero, abril, julio y octubre.

La falta o incumplimiento en la entrega de algún reporte o actividad ilícita cometida, la institución financiera será acreedora a multas establecidas por los reguladores locales, a continuación, se muestran las multas a los cuales pueden ser acreedores, cabe mencionar que dicha información está sujeta a cambios y/o actualizaciones realizadas por los mismos reguladores locales.

INFRACCIONES Y/O SANCIONES.

INFRACCIÓN	MULTA
Realizar operaciones con clientes o usuarios que se encuentren en la lista de personas bloqueadas.	10% al 100% del monto del acto, operación o servicio que se realice.
No reportar alguna operación inusual.	10% al 100% de la operación.
No entregar reporte de operaciones relevantes, internas preocupantes**.**	10,000 a 100,000 días de salario.
Inadecuado conocimiento de sus clientes (metodología KYC)	10,000 a 100,000 días de salario.
No resguardar, ni garantizar la seguridad de la información y documentación relativa a la identificación de sus clientes**.**	10,000 a 100,000 días de salario.
No registrar en su contabilidad cada una de las operaciones u actos que celebren.	5,000 hasta 50,000 días de salario según el sector.
No establecer medidas y procedimientos para prevenir operaciones para la comisión, de los delitos de lavado de dinero y financiamiento al terrorismo.	5,000 hasta 50,000 días de salario según el sector.
No conservar la información y documentación relativas a la identificación de sus clientes y usuarios, por lo menos 10 años.	5,000 hasta 50,000 días de salario según el sector.

FUENTE: CNBV

Capítulo 4 Prevención de fraude en las áreas operativas de una institución bancaria.

4.1 Definición de fraude.

Toda organización está expuesta a que personas externas o internas lleven a cabo un fraude, lo cual conlleva a la institución a un riesgo financiero, legal e incluso reputacional, es por ello, que el control interno de la institución y sus directivos analicen el nivel de riesgos a los cuales pueden estar expuestos, con la finalidad de establecer estrategias y las medidas de control a implementar para mitigar las consecuencias de ello.

Podemos definir el fraude como el uso o apropiación deshonesta de bienes, recursos, servicios o beneficios.

Association of Certified Fraud Examiners indica que el fraude es aquel acto intencional o deliberado de privar a otro de una propiedad, dinero, etc. por medio de la astucia, el engaño u otros actos desleales.

De acuerdo a Andrew Nelson fraude consiste en alguna práctica engañosa plan preconcebido con la intención dolosa de privar a otro de sus derechos, o en alguna forma causarle perjuicios.

De acuerdo a lo anterior, podemos decir que el fraude es aquel acto deshonesto que realiza una o varias personas, puede que obtenga un beneficio personal o simplemente busque generar una perdida para la institución. Un ejemplo de ello es cuando una persona proporciona información falsa o que intencionalmente resguarda información con la finalidad de engañar al propietario de los recursos en cuestión.

Las principales características del fraude son:

1. Abuso de confianza.
2. Se realiza mediante engaños.
3. Generalmente no se utiliza la violencia o fuerza física.
4. Puede obtenerse una ventaja económica o de manera personal.
5. Puede ser solo un individuo o varios.

Además del impacto financiero que puede tener la institución ante un fraude existen afectaciones secundarias que también perjudican severamente, por ejemplo:

1. Mala imagen de la institución.
2. Baja de moral e inquietud del personal.
3. Pérdida de clientes.
4. Desconfianza de proveedores.
5. Pérdida de socios y/o accionistas.

Donald Cressey's generó un modelo en el cual hace mención de los factores que contribuyen a que una persona cometa fraude. Cabe mencionar que los conceptos mencionados pueden variar de nombre de acuerdo a la cultura de control gestionada por cada institución.

TRIÁNGULO DEL FRAUDE.

Necesidad: es aquella situación que motiva al individuo a cometer el fraude, por ejemplo:

a) Problemas financieros.
b) Adicción(es).
c) Deseos de un status vida superior (casa, auto de último modelo, viajes, etc.).
d) Necesidad financiera inesperada.
e) Presión por alcanzar objetivos de productividad.

Racionalización: en esta etapa la persona que está a punto de cometer el fraude, realiza cierto de grado de justificación y genera ciertas afirmaciones que le ayuden a tomar su decisión, por ejemplo:

a) Solo estoy tomando un préstamo.
b) Me lo merezco.
c) No me pagan lo suficiente.
d) Mi familia lo necesita.
e) No hace daño a nadie, la compañía tiene mucho dinero.

Oportunidad: es el método por el cual la persona puede cometer el fraude, éstos pueden ser:

a) Debilidades y/o ausencia del control interno.
b) Acceso a sistemas y/o información confidencial.
c) Exceso de confiabilidad.
d) Falta de revisiones y/o auditorías.

Tener el conocimiento de estos factores es de gran ayuda ya que, al percatarse oportunamente de la existencia y combinación de las situaciones mencionadas anteriormente, sabremos que existe un alto nivel de riesgo por lo cual la institución se encuentra en situaciones propensas al fraude, debido a ello el área de control y los directivos deberán de realizar un estudio a cada área y personal perteneciente a ella, para definir estrategias, programas, políticas, capacitaciones, etc. que fortalezcan los procesos relacionados reduciendo la posibilidad de que se susciten irregularidades.

4.2 Clasificación de fraude.

La institución puede ser atacada por personas internas o externas, es por ello necesario conocer de qué manera efectúan el fraude para estar prevenidos ante ello y poder mitigar la afectación.

Fraude interno o también conocido como fraude laboral es ejecutado por un ejecutivo, gerente, socio o empleado temporal que forman parte de la institución, tomando como ventaja su puesto, la información que administran, los sistemas a los cuales tienen acceso. La característica principal de este tipo de fraude es que se ejecuta a través de una persona de la institución que tiene amplio conocimiento del proceso y las debilidades existentes en las medidas establecidas por el área del control y la alta dirección, cabe mencionar que este fraude puede ser ejecutado sin importar los niveles (Dirección, analistas, personal de seguridad, etc.), o la antigüedad del empleado.

Este fraude puede ser resultado de la continua imposición de los supervisores para el logro de los resultados, o cierta desmotivación del empleado que lo incita a cometer el fraude hacia la institución obteniendo un beneficio económico o simplemente una venganza o desquite en contra de la institución.

Desafortunadamente este tipo de fraude no es tan fácil detectarlo de manera inmediata u oportuna debido a que puede existir colusión entre empleados y personas externas; las posiciones directivas suelen ser más sensibles al fraude ya que poseen de facultades privilegiadas, a continuación se enlista algunas maneras en la que los empleados pueden cometer fraude, es por ello la importancia de conocerlas para que el área de control interno y el oficial de administración de fraude pongan atención a ellas:

1. Robo de datos, el empleado puede buscar obtener alguna ganancia al vender o utilizar información de clientes, información financiera de la institución o estrategias de productos y/o servicios nuevos.
2. Abuso de puesto, se puede llevar a cabo mediante las autorizaciones de bonos que no le correspondían al empleado en cuestión, coordinarse en conjunto con personas de otras áreas para obtener aumentos de sueldos no merecidos.
3. Robo de identidad, el empleado accede a la cuenta de un cliente sin autorización y lleva a cabo transacciones a su nombre no autorizados, adueñándose de los activos del cliente.
4. Manipulación de datos, se puede llevar a cabo mediante la declaración falsa de la situación financiera de la institución, con la finalidad de conseguir inversionistas, vender acciones, solicitar préstamos, etc.
5. Corrupción, este método implica también a personal externo ya que estos pueden ofrecer regalos, beneficios, alguna suma monetaria al personal que forma parte de la institución para que le sea proporcionada cierta información.

Para este tipo de fraude es importante que el área de control y cada una de las personas dentro de la organización sin importar el nivel, es decir desde el operativo hasta directivos presten atención a las Banderas Rojas o “Red Flags”, los cuales son aquellos comportamientos o acciones que pueden indicar que una persona es propensa a realizar fraude.

El Fraude externo es el resultado de las acciones fraudulentas contra la institución que son realizadas por personas ajenas, por ejemplo; proveedores, clientes, empresa competidora, delincuentes, etc.

Para prevenir el fraude también debe mirarse hacia el exterior de la institución, es decir saber con quién tenemos relaciones comerciales, involucrando a nuestros proveedores y clientes como aliados para la lucha contra el fraude, concientizándolos de las consecuencias que pueden existir para ambos. El área de control interno o el oficial contra el fraude deben de dar a conocer a los proveedores y clientes el canal de denuncia contra el fraude, de esta manera pueden reportar aquellas actividades que ellos consideren sospechosas de fraude y lleguen a perjudicar la relación comercial con la institución.

Algunos tipos de fraude externo son:

1. Robo de identidad, esta actividad puede ser efectuada por medio de páginas web falsas, virus informáticos, robos de correspondencia.
2. Fraude por medio de tarjetas, lo más común en este método es por medio de robo y la falsificación, en la cual la persona se hace pasar por otra para realizar compras o disposición de efectivo de las tarjetas en cuestión.
3. Fraude por solicitud, sin las medidas correctas de control la institución puede caer en el error de proporcionar deliberadamente información incorrecta a la solicitud de una cuenta.
4. Fraude por fallas de seguridad en los sistemas, actualmente el avance tecnológico se va desarrollando día a día, lo cual hace una oportunidad de cometer fraude si no se tiene las medidas correctas pueden existir ataques informáticos, para el robo de información.

4.3 Administración de controles para la prevención de fraude.

Para la batalla contra el fraude es importante la aplicación de los controles internos, así como también la comunicación y aplicación de la integridad y valores éticos a cada uno de los empleados de la organización.

Para una correcta ejecución de los controles que ayuden a prevenir el fraude es necesario la participación de las 3 líneas de defensa recordando el principal papel de cada una de ellos, es decir:

1. Primera línea de defensa: el área de negocio y/u operativa es la encargada de conocer y prevenir los riesgos de fraude que podrían ocurrir en cada una de sus áreas, por lo que deben operar con los controles que les ayuden a mitigar el riesgo, para ello debe de apoyarse con la segunda línea de defensa para el diseño e implementación adecuada de los controles.
2. Segunda línea de defensa: el área de prevención del fraude se encuentra dentro de la segunda línea de defensa y tiene la responsabilidad de la elaboración, actualización y aplicación de los controles y/o políticas contra el fraude, proporcionando soporte a las áreas de negocio y/u operativa.
3. Tercera línea de defensa: es el área de auditoría interna que se encarga de realizar las revisiones y evaluaciones a las dos líneas de defensa previamente señaladas respecto a la correcta aplicación de los controles diseñados, así mismo debe de dar a conocer a la dirección de manera autónoma los resultados de dichas revisiones.

Las tres líneas de defensa deben de aplicar el principio REAF (siglas en ingles)

Recognize (Reconocer)
Examine (Examinar)
Act (Actuar)
Follow–up (Seguimiento)

1. Reconocer: darse cuenta de aquellas transacciones inusuales o brechas que existan en el proceso.
2. Examinar: cada empleado y supervisor debe tomarse su tiempo para revisar cada operación antes de ser aprobado o enviado.
3. Actuar: en caso de existir alguna actividad sospechosa, es importante que se detenga la transacción y escale sus inquietudes.
4. Seguimiento: se deberá dar continuidad a todos los casos escalados, asegurándose que se han resuelto correctamente.

Como se puede observar, la importancia de conocer y aplicar este principio es que nos detalla las acciones a seguir para combatir y prevenir el fraude, dichas acciones tratan de ser lo más accesible posible para que sean aplicados a todos los niveles de la institución, por lo cual se debe considerar darle a conocer a todos los empleados el principio REAF y el significado de sus cuatro componentes, de esta manera podemos reforzar el conocimiento de cada empleado para la lucha contra el fraude.

Debido al constante desarrollo de métodos y tecnologías que favorecen las modalidades en las cuales se pueden realizar fraude, las probabilidades de que una institución puede ser atacada incrementan día a día, afortunadamente en la actualidad existe mucha información y/o modelos a seguir que les puede ayudar a fortalecer sus medidas de control.

Dependerá de la institución y su cultura que tipo de modelo y controles puede implementar de acuerdo a sus necesidades; por ejemplo, el Committee of Sponsoring Organizations of the Treadway Commission o también conocido como COSO por sus siglas en ingles dio a conocer un modelo cuya finalidad es que las instituciones puedan combatir y protegerse del fraude ya sea de origen interno o externo, ello se puede lograr por medio de la aplicación de 5 componentes que nos muestra el siguiente diagrama. La recomendación principal de COSO es que una vez que los componentes sean aplicados se realice constantemente una evaluación exhaustiva del mismo, esto les permitirá observar sus riesgos en control interno y si el modelo es efectivo a sus procesos, de no ser así es recomendable que se realice los cambios y/o ajustes que la institución considere necesarios.

MODELO DE GESTIÓN DE RIESGO – COSO.

Como podemos observar este modelo proporcionado por COSO está basado en medidas básicas y sencillas de control, para que pueda ser implementado en cualquier institución.

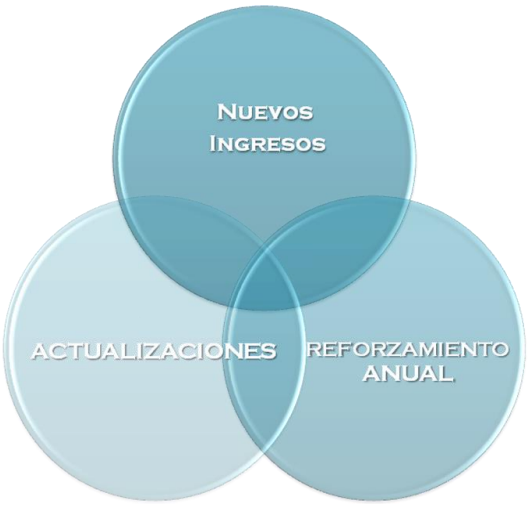
4.4 Responsabilidad del personal del área de operaciones para la prevención de fraude.

Al contratar a un empleado, se espera que sea una persona honesta y con las mejores prácticas de valores posibles, consideremos que un empleado no nos puede garantizar que no se presenten actos fraudulentos, sin embargo, su reacción cuando surjan sospechas de fraude debe de ser lo más adecuada y pronto posible.

El empleado puede ser considerado como el eslabón más fuerte de la cadena anti fraude, al ser dueño de sus procesos, conoce las debilidades y fortalezas en cada una de sus tareas. El método más rápido de detectar un fraude interno y tener oportunidad de detenerlo, es mediante el reporte del mismo personal de la institución.

Por ello es de gran importancia compartir a los empleados el código de conducta esperando que actúen de acuerdo a los valores esenciales, creando confianza para expresar sus preocupaciones, inquietudes, sospechas de violaciones de las políticas, etc.

El entrenamiento constante a los empleados también es una parte fundamental, ya que de esta manera tendrán el conocimiento de cómo actuar en sospecha de alguna situación de fraude, así como también los concientizará respecto a las consecuencias que pueden existir al momento de cometer fraude; el entrenamiento se puede otorgar en los siguientes casos:



Las principales responsabilidades a considerar son:

1. Actuar con honradez.
2. Denunciar cualquier acto de sospecha de fraude.
3. Reportar debilidades de los controles y/o programa anti fraude detectadas en sus actividades.
4. No hacer favores a compañeros y/o supervisor a solicitudes que sean consideradas sospechosas de fraude, por ejemplo, transferencias sin previa aprobación, proporcionar información confidencial de clientes, etc.
5. No proporcionar usuario y/o contraseña para el ingreso a sistemas a personal ajeno a las funciones.
6. Aceptar y asumir la responsabilidad de sus actividades asignadas de acuerdo a la segregación de funciones previamente estipuladas.
7. Participar en las capacitaciones contra el fraude proporcionadas por el oficial de cumplimiento, el área de control, etc.
8. Resguardar la información de acuerdo a lo establecido por las políticas, así como también proporcionar toda la documentación solicitada por el oficial de fraude.

No olvidemos que la responsabilidad de combatir el fraude es de todos los empleados sin importar niveles, es decir los directivos, supervisores y/o representantes de cada área deben de cumplir con cada política, programa anti fraude, código de conducta, etc., de esta manera garantizamos que los demás empleados tienen un ejemplo a seguir y sobre todo podrán visualizar el compromiso existente para prevenir y combatir el fraude.

4.5 Programa de administración de fraude.

La aplicación de un programa de administración de fraude nos permite combinar aspectos culturales y conductuales de la organización y cada uno de los empleados, cuando la institución genera un ambiente en el que los empleados actúen con ética genera una actitud de compromiso, el programa también aplica controles internos que fortalezcan a la institución y ayudan a mitigar el fraude. La formalización de un programa anti fraude tiene como beneficio mandar un mensaje al personal, socios, accionistas, clientes, y proveedores que en la institución se preocupan por el bienestar de todos y no se toleran acciones fraudulentas o ilícitas.

Los principales objetivos en la aplicación de un programa para la prevención del fraude son:

1. Establecer un sistema de gobierno para la administración del riesgo contra el fraude.
2. Definir roles y responsabilidades.
3. Establecer medios de comunicación, con el objetivo de mantener constante interacción y actualización de los estándares requeridos para los controles contra el fraude.
4. Asignar canales de denuncia para reportar sospechas o intentos de fraude, desaparición inexplicada de fondos o valores u otras actividades bajo sospechas.
5. Realizar programas de capacitación en materia de concientización sobre el fraude.

A continuación, se muestra el ciclo de un programa anti fraude.

1. La prevención es la primera línea de actuación en un programa anti fraude ya que nos ayudará a mitigar el riesgo implementando políticas, manuales, etc.

2. Detección, en este elemento es importante que se realice la evaluación y supervisión de manera continua la cual nos ayudará a percibir las fallas en los controles, ya que ello dependerá para iniciar una investigación y/o cambios en las políticas previamente establecidas.

3. Investigación una vez que se haya recibido un reporte sobre actividades sospechosas es importante que la institución tenga un protocolo de actuación formal, para iniciar a indagar de manera detallada; es decir realizar entrevistas, recolección de evidencias, documentos internos, fuentes externas, etc.

4. Las lecciones aprendidas se puede obtener conocimiento de aquellas experiencias o intentos de fraude a la institución, también puede adquirir como experiencia lo ataques que hayan recibido otras instituciones, de esta manera la organización podrá reforzar su programa anti fraude.

5. Entrenar al personal, la institución debe de implementar un programa de capacitación al personal, que ayude a robustecer y mitigar el riesgo de fraude.

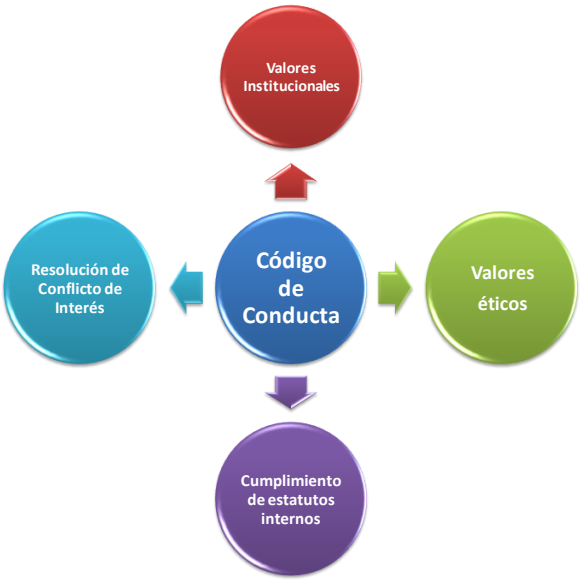
6. Para concientizar al personal se debe de mantener constante comunicación con los empleados, respecto a las consecuencias resultantes de los fraudes.

Algunos elementos que podemos considerar en el programa de fraude son:

1. Políticas para la prevención de fraude.
2. Evaluación del riesgo de fraude.
3. Código de conducta.
4. Roles y responsabilidades con las tres líneas de defensa.
5. Nombramiento de un oficial de administración de fraude.
6. Concientizar a los empleados con una conducta de honestidad, transparencia y trabajo en equipo.
7. Crear medios por los cuales los empleados puedan reportar alguna actividad sospechosa de manera anónima.
8. Procedimientos para documentar las deficiencias identificadas.
9. Comunicación con los directores indicando las deficiencias y mejoras pertinentes.

El ¿por qué? incluir el código de conducta en un programa de prevención del fraude, es debido a que este establece las expectativas que la institución espera del empleado en cuanto a su comportamiento y valores esenciales, también ayuda a generar la confianza en los empleados para externar sus inquietudes o dudas en materia de ética y a reportar cualquier tipo de sospecha, esto lleva a un clima laboral basado en la comunicación y el respeto a todos los niveles de la institución; resumiendo si la organización fomenta una cultura de ética, confianza y respeto, hacia los empleados, proveedores, clientes, etc. El trato de cada uno de ellos será reciproco.

ELEMENTOS DEL CÓDIGO DE CONDUCTA.



Es de suma importancia mantener la actualización del programa anti fraude ya que mientras más fuertes y solidas son las políticas, así como el conocimiento de las sanciones que pueden aplicarse por la ejecución de fraude, se disminuirá la disponibilidad, facilidad e inquietudes para cometer un fraude.

Dentro del programa de administración de fraude el área de control interno, oficial de fraude y la alta dirección en conjunto deben de trabajar en crear una cultura de cero tolerancia al fraude, es decir en ellos recae la responsabilidad de fortalecer las políticas anteriormente mencionadas, manteniendo una constante comunicación con todos los empleados, así como también darles a conocer las actualizaciones que se realicen en cuanto a las políticas, medidas de control que enfrenten al fraude de todas las maneras posibles, ya sea fraude económico, robo de documentación y /o datos, falsificación de información, etc.

4.6 Importancia de la figura del oficial de fraude.

En los capítulos anteriores se ha hecho mención de la necesidad de segregación y asignación de funciones, para combatir el fraude es de suma importancia que la institución haga el nombramiento de un “Oficial de Fraude” esta persona será el encargado de la prevención del fraude, realizando exámenes y evaluaciones de la efectividad del control interno, también es el responsable de la implementación de un programa eficaz y mantener constante contacto con la Dirección para dar a conocer las debilidades y fortalezas de la institución.

El oficial de fraude debe tener la experiencia para identificar los indicadores de fraudes, así mismo se le debe de otorgar la autoridad adecuada para efectuar las revisiones y correcciones necesarias. Las cualidades significativas del oficial es que sea una persona ética, integra y objetivo.

El objetivo principal de un oficial de cumplimiento es evaluar constantemente todos los componentes relacionados que la institución aplica contra el fraude, con la finalidad de asegurar la efectividad y mejora continua de los controles, políticas, programas, códigos de conducta etc.

Algunas de sus funciones principales pueden ser:

1. Asegurar el continuo monitoreo de las políticas, procesos y controles aplicados a cada uno de ellos.
2. Dirigir actividades y cerciorarse del cumplimiento de ellas, así como también la elaboración y entrega de reportes solicitados por los reguladores locales, con la finalidad de evitar sanciones significativas.
3. Ejecutar el programa anti fraude.
4. Verificar el cumplimiento y actuaciones del personal respecto al código de conducta.
5. Presentar informes periódicos a la Dirección sobre la efectividad del programa anti fraude, políticas, procedimientos, etc.
6. Dar soporte en las actualizaciones del programa anti fraude, políticas, código de conducta, etc.
7. Proporcionar apoyo y orientación a los empleados que tengan cuestionamientos sobre el programa anti fraude, políticas, código de conducta, etc.
8. Desarrollar cursos de capacitación, volantes y otro material para sensibilizar a los empleados sobre el programa anti fraude.

Es importante que los directivos den a conocer a los diversos empleados la importancia de trabajar en conjunto con el oficial de fraude, ya que de esta manera la institución se está fortaleciendo contra las amenazas externas o internas.

4.7 Investigaciones y lecciones aprendidas.

De acuerdo a lo que se ha mencionado a lo largo del capítulo, las amenazas de fraude son constantes y crecientes ya que a menudo se usan trucos de confianza que explotan la psicología humana y otras tácticas de manipulación para favorecer los planes de fraude.

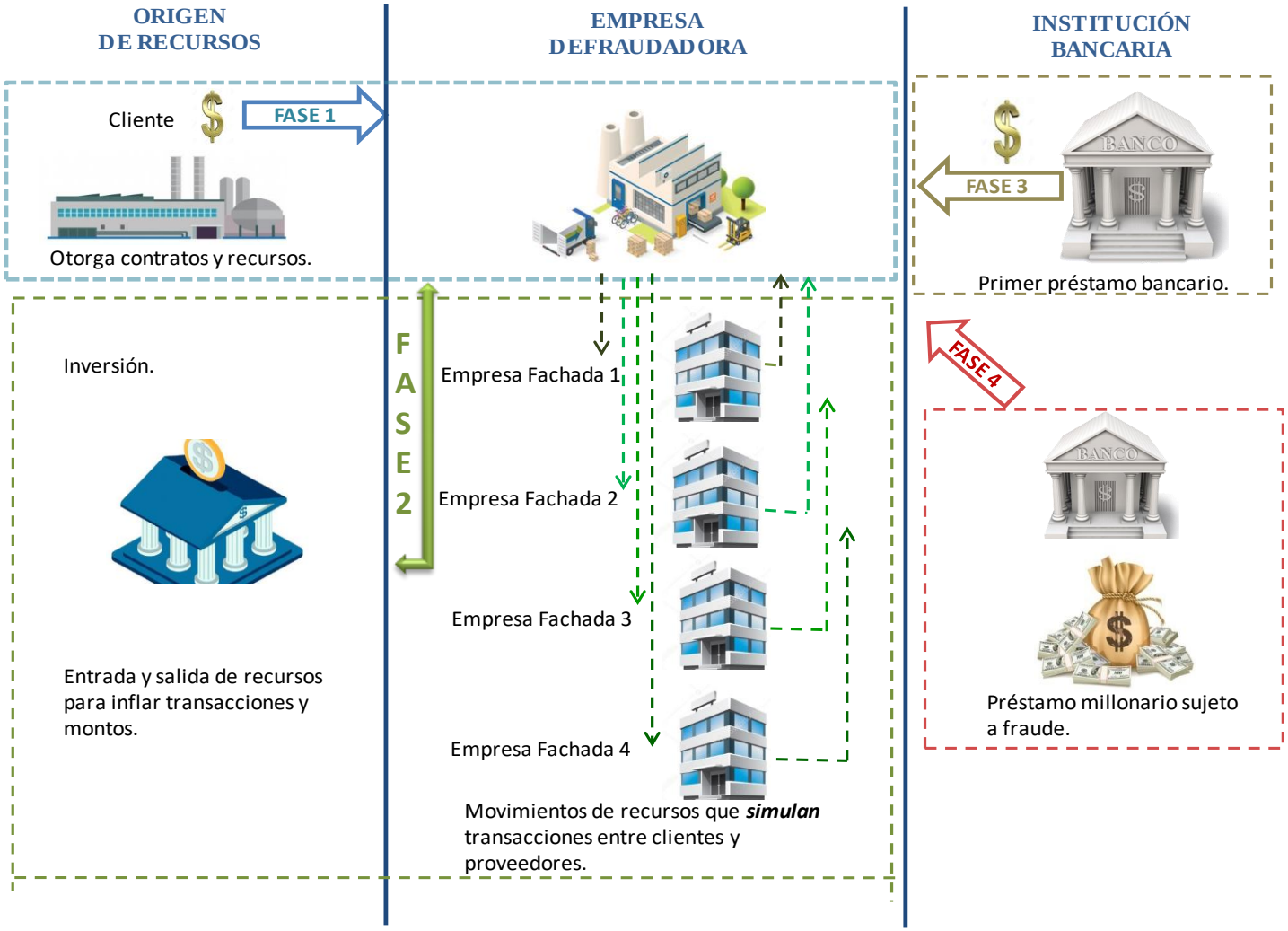
Debido a ello surge la importancia de combatirlo, manteniendo una cultura de control que fortalezca la seguridad de la institución; sin embargo, pueden existir eslabones débiles los cuales pueden ser oportunidad para que la institución sea víctima de dichos actos. Por ello las instituciones deben de realizar investigaciones una vez que exista una sospecha de posible fraude o actos inusuales realizados por los mismos empleados de la institución.

Otro método de aprendizaje para las instituciones, es el conocimiento del exterior, es decir mantenerse actualizados sobre actividades fraudulentas que se hayan llevado a cabo hacia una institución ajena, personas etc., de esta manera podrán ver los métodos y fallas que cometió la institución o persona(s) en cuestión, convirtiéndose en una lección aprendida para no cometer los mismos errores u omisiones, y estar preparados para combatir el fraude.

Es recomendable que los directivos, el área de control y oficial de fraude lleven a cabo reuniones para realizar una retroalimentación y la importancia de adquirir información actualizada de defraudadores, así como también perfiles de perpetradores y método de la elaboración del fraude, con la finalidad de robustecer la cultura de control.

A continuación, se mencionarán ejemplos de fraudes internos y/o externos que pueden ser cometidos en contra de las instituciones si no se tiene las consideraciones necesarias como, las medidas de controles eficientes, omisiones o desconocimiento de los empleados de la misma institución, los cuales pueden ser de alto riesgo para ser víctima de fraude.

CASO 1 Fraude externo



A continuación, se mencionará el detalle de cada fase en la cual se llevó a cabo el fraude contra de la institución bancaria.

Fase 1 Origen de recursos:

La institución defraudadora obtiene sus recursos reales (legales) de un cliente al cual ofrece sus productos/servicios y existen contratos, facturas comunes como en cualquier operación compra – venta.

Fase 2 Inversión y empresas fachadas:

Debido a la obtención de los recursos que tiene la empresa en la fase uno, realiza una inversión en una institución bancaria, a la cuál le envía parte de los recursos, que posteriormente serán regresados a la empresa defraudadora, el objetivo es mostrar movimientos en la cuenta, al mismo tiempo la empresa defraudadora comienza a realizar la dispersión de los recursos a diferentes empresas fachadas[18] siempre devolviendo los recursos a la empresa defraudadora, es decir; la empresa defraudadora envía recursos a la empresa fachada 1, una vez que esta lo obtiene refleja dichos movimientos en su contabilidad y una vez finalizado el proceso, la empresa fachada 1 regresa la misma cantidad de recursos que recibió a la empresa defraudadora; este ejercicio lo realiza con las cuatro empresas fachadas que fueron creadas. Cabe mencionar que los recursos que son enviados de una empresa a otra, así como la inversión, siempre son los mismos; este tipo de estrategia es utilizada solo para inflar los estados de cuenta de la empresa defraudadora, ya que a simple vista demuestra que obtiene recursos de diversas fuentes, sin reflejar que es lo mismo con lo que inició.

Fase 3 Préstamo bancario que puede ser liquidado:

La empresa defraudadora acude a una institución bancaria diferente en la cual realizó su inversión, su objetivo con este segundo banco es el solicitar un préstamo, teniendo como estrategia requerir una cantidad que pueda liquidar; una vez obtenido el préstamo por parte del banco, la empresa defraudadora empieza a realizar las mismas operaciones que en la fase dos, es decir, los recursos prestados por el banco también fueron dispersados a la inversión y las diferentes empresas fachadas, siempre regresando el recurso a la empresa defraudadora, con el mismo objetivo de la fase dos; que es el inflar sus estados de cuenta mediante los diversos movimientos realizados con el préstamo bancario, una vez que dichos movimientos se ven reflejados en sus libros contables y estados de cuenta, la empresa defraudadora liquida el préstamo que le otorgo el banco con el fin de ganar confianza y mantener buen historial crediticio con esa institución financiera.

[18] Empresa Fachada: Son oficinas virtuales que no tienen empleados, empresas creadas para cometer fraude.

Fase 4 Ejecución de fraude:

Debido al buen historial crediticio que generó la empresa defraudadora al liquidar su préstamo con el banco y a los grandes movimientos de recursos en sus cuentas, dicha empresa acude nuevamente para solicitar un préstamo millonario el cual será sujeto a fraude, para poder obtenerlo, la empresa defraudadora puede presentar la siguiente documentación:

1. Facturas apócrifas (de su cliente real y de las empresas fachadas): para demostrar que mantiene negocios con sus clientes y le está otorgando nuevos proyectos, de los cuales recibirá el pago de cada uno generándole ganancias con las cuales podría liquidar el préstamo.
2. Estados de cuenta que fueron inflados con los mismos recursos, para demostrar que tiene la liquidez suficiente.

De esta manera el banco que será sujeto a fraude, con la confianza obtenida, le otorga el préstamo millonario a la empresa defraudadora, y así es como logra su objetivo obteniendo los recursos millonarios que no serán liquidados en el futuro.

Como podemos observar este tipo de fraude fue externo, pero fue logrado debido a fallas y/o debilidades que cometió el banco.

Fallas de la institución bancaria:

1. Facturas apócrifas: el personal de la institución bancaria no dedicó el tiempo necesario para realizar la validación de las facturas presentadas, si hubieran revisado detalle como:

a) Número de folio de la factura coincidiera con la numerología expedida por el SAT.
b) Existencia física de las razones sociales descritas en las facturas, tiempo de vida en el sector comercial, sitios web y correspondencia entre estos.

De esta manera hubieran observado que las facturas presentadas eran falsas, siendo un punto en contra de la empresa defraudadora para no otorgarle el préstamo.

2. Confianza excesiva: el personal de la institución bancaria desde los operativos hasta la alta dirección confió en el renombre, buen historial e importancia que decía tener la empresa defraudadora.

3. Omisión de aprobaciones: esta falla se encuentra ligada con la mencionada anteriormente, ya que por la confianza que tenía el personal del banco con la institución defraudadora, pasaron por alto documentación que tenía que ser aprobada por personal directivo para el otorgamiento del préstamo.

4. Falta de verificación de proveedores y/o empresas fachadas: la institución bancaria no realizó el proceso de validar que la información proporcionada por la empresa defraudadora fuera cierta, para ello tenía que indagar la relación que decía tener con sus diversos proveedores:

a) Facturas verificando con el SAT: solicitar documentación que demostrara la relación comercial con las empresas fachada y su veracidad.

Estos fueron algunos puntos que la institución bancaria debió de realizar para evitar ser víctima de fraude.

Recordemos que las omisiones o exceso de confianza facilitan la ejecución de un fraude, el cual, siempre lleva algún impacto en contra de la institución bancaria, por ejemplo:

1. Impacto financiero, ligado a perdida de utilidades y desmotivación del personal.
2. Multa del regulador local (CNBV) por incumplir con procedimientos de control interno contra el fraude.
3. Despidos de personal desde alta dirección hasta nivel operativo por la omisión de controles.
4. Impacto a la imagen reputacional del banco.

Acciones después del fraude.

Como hemos observado este banco no pudo evitar el ser víctima de fraude, convirtiéndose esta mala experiencia en una lección aprendida, permitiendo analizar a detalle sus errores y fortalecerlos; algunas sugerencias de acciones que puede tomar en cuenta el banco para fortalecer sus controles son:

1. Concientizar al personal sobre el correcto cumplimiento de los procesos anti fraude.
2. Fortalecer sus cursos de entrenamiento a todo el personal incluyendo a directivos.
3. Fortalecer la medida de control “Maker – Cheker” a todos los niveles.
4. Sin hacer distinción de clientes, todo proceso debe de cumplir con las aprobaciones pertinentes sin falta alguna, de lo contrario no deberá de realizarse ninguna transacción o préstamo de recursos.
5. El oficial de fraude, el departamento de control y los responsables de cada departamento deberán agendar de manera mensual o bimestral la revisión de sus procesos, con la finalidad de verificar el cumplimiento del 100% de las medidas implementadas contra el fraude.

CASO 2 Fraude interno

Cliente

Instruye transferencia de fondos a terceros.

Persona física - Cliente 1

$ 13,851.50

Persona moral - Cliente 2

$ 30,529.95

Persona física - Cliente 3

$ 2,616.19

Persona moral - Cliente 4

$ 78,302.75

Empleados de la Institución Bancaria

Recibe instrucciones

Recibe y valida cada una de las instrucciones enviadas por los clientes

Liquida las instrucciones indicadas por el cliente.

Cliente 1
$ 13,851

Cliente 2
$ 30,529

Cliente 3
$ 2,616

Cliente 3
$ 78,302

Empleado trunca las transferencias de los clientes a números cerrados, las fracciones, son enviadas a cuentas de un tercero (cómplice)

Cuenta de un tercero

C1 **$ .50**
C2 **$ .95**
C3 **$ .19**
C4 **$ .75**
$2.39

Fraude aproximado por un equivalente a **300 transacciones por día**

A continuación, analizaremos de qué manera se llevó a cabo el fraude que muestra el diagrama anterior, y cuáles fueron las fallas u omisiones cometidas.

Fase 1: Solicitud de transacciones.

Día a día los clientes (personas físicas y morales) envían a la institución bancaria instrucciones de transferencias de recursos para ello es necesario que envíen un formato detallado en el cual indiquen cuenta, monto, beneficiario y fecha de la operación.

Fase 2: Validación de información.

La institución bancaria tiene asignado a personal el cual tiene como sus principales funciones revisar las instrucciones enviadas por el cliente; algunos aspectos que debe validar son:

1. Nombre del cliente.
2. Nombre del beneficiario (quien recibirá el recurso)
3. Cotejar que la firma e información del cliente coincida con las bases en la que tiene la identificación de cada uno de ellos.

Una vez que se haya cotejado la información y sea correcta, el personal de validación deberá de enviar la instrucción al área operativa correspondiente para ejecutar la transacción.

Fase 3: Ejecución del fraude.

La instrucción es recibida por el personal encargado de liquidar los pagos, quien lleva laborando varios años en el banco y es auto gestionable, es decir, no tiene supervisor que valide las transacciones realizadas, es un proceso monótono y a través del tiempo se ha dado cuenta de sus debilidades.

El empleado realiza la transacción solicitada por los clientes; sin embargo las cifras enviadas a la cuenta del beneficiario son cantidades cerradas, en paralelo envía los centavos a una cuenta que aperturó a nombre de otra persona; es decir si el cliente solicitaba pagar a un beneficiario la cantidad de $13,851.50 MXN, el empleado transfería al beneficiario solo $13,851.00, enviando los .50 centavos a una cuenta que él o un familiar aperturó, este tipo de ejercicio lo realizaba diariamente con todas las instrucciones que recibía.

Con el objetivo de fortalecer sus medidas de control, el banco implementa la estrategia de “Ausencia Obligatoria”, está consiste, en que todo empleado del banco que tenga funciones relacionadas con movimiento de dinero, afectaciones a libros contables deberán tomar un periodo vacacional de 10 días seguidos; debido a esta estrategia se le solicita al área asignar un “back up” (empleado encargado de cubrir al personal ausente). Durante el periodo en el que el “back up” realiza las funciones, el área de contabilidad se percata que se están recibiendo varios registros de operaciones con centavos, lo cual no sucedía en los años anteriores; estas situaciones llamaron la atención de dirección, por lo cual se solicitó realizar una auditoría interna, y en ese

momento se vio reflejado el fraude por la desviación de centavos que realizaba el empleado.

De acuerdo a lo analizado anteriormente, nos podemos percatar que se cometió fraude interno; las principales fallas y/u omisiones que cometió el banco son:

1. Falta de “Maker – Checker”: al no existir un supervisor que validara la instrucción del cliente contra lo que era enviado de acuerdo a la instrucción; fue una oportunidad para que el empleado se confiara de que nadie revisaba su trabajo y cometiera el fraude.
2. Falta de proceso “call back”: en este tipo de operaciones, el área debió de haber implementado el proceso de validación vía telefónica con el cliente, con la finalidad de confirmar la cuenta y el importe solicitado.
3. Falta de conciliaciones: el área no llevaba a cabo conciliaciones al cierre del día ni de manera mensual, lo que impedía visualizar la cantidad que era instruida contra la cantidad que se registraba en los sistemas contables.
4. Falta de auditoría interna periódica: el área de control interno y personal directivo omitió el realizar revisiones, facilitando que nadie se percatará de los movimientos que realizaba el empleado.

Como podemos observar, la falta de controles eficientes en la institución además de ser presentar un riesgo externo, también implica un riesgo interno ya que los empleados pueden aprovechar las debilidades del banco para obtener sus propias ganancias.

Acciones después del fraude.

Después de esta mala experiencia que tuvo la institución, le quedó como una lección aprendida, que también existe un riesgo dentro de su empresa, por lo cual tendrá que fortalecer los siguientes puntos:

1. Distribución y fortalecimiento del código de conducta a todos los niveles de la institución.
2. Implementación de Maker – Checker en todos los departamentos.
3. Implementación de firmas mancomunadas para cantidades superiores de dinero, es decir, la participación de un tercer empleado generalmente de nivel dirección adicional al “Maker-Checker” para realizar la autorización.
4. Los responsables de cada departamento, el oficial de fraude y área de control deberán de trabajar en conjunto para llevar a cabo las auditorias de manera mensual.
5. Aquellos departamentos en las que sus funciones principales conlleve la manipulación de dinero, deberán de realizar una conciliación diaria, y esta debe ser reportada al área de contabilidad, con sus respectivas firmas de aprobación.
6. Implementar el proceso de “call back” con el cliente previo a su ejecución, con la finalidad de corroborar la información y a su vez obtener su visto bueno, teniendo como soporte que la transacción se realizó de manera correcta.

CASO 3 Fraude a clientes de instituciones financieras (por teléfono y vía electrónica)

Defraudador

Cliente

Fase 1

El defraudador llama al cliente para notificarle que recibió un "depósito" considerable en su cuenta y requiere de su aprobación.

Fase 2

El cliente desconcertado pregunta su procedencia, sin embargo el defraudador comenta que no cuenta con esos detalles, reitera que es un beneficio para el cliente y no cuenta con información de origen del recurso, haciendo el comentario que una vez que autorice, el cliente podrá obtener detalle del origen; por lo tanto esté decide proporcionar su número de usuario y contraseña ya que se trata de un depósito y no de un cobro o retiro que es lo que comúnmente se utiliza para defraudar vía telefónica.

Fase 3

El defraudador genera un alta de cuenta a un tercero (es decir a él mismo), adicionalmente programa una transferencia por un monto total a la cantidad que el cliente tiene en sus cuentas, para finalizar le indica al cliente que su depósito caerá en un tiempo determinado, para que ingrese a su cuenta y confirme que el depósito se haya realizado

A continuación, analizaremos de qué manera se llevó a cabo el fraude que muestra el diagrama anterior, y cuáles fueron las fallas u omisiones cometidas.

Fase 1: Contacto de defraudador con el cliente.

El defraudador llama al cliente, haciéndose pasar por ejecutivo del banco, notificándole que el cliente ha recibido un depósito por un monto considerable (ejemplo $100,000.00) en su cuenta, explicando que la finalidad de su llamada, es para autorizar y liberar el depósito. El cliente desconcertado puede autorizar el depósito sin cuestionar o bien preguntar el origen del depósito. Ya que no esperaba recibir dicho monto, en este caso, el defraudador indica que es solo un empleado y desconoce el origen del recurso, solo necesita la autorización del cliente por medio de las contraseñas.

Fase 2: Solicitud de información y contraseñas.

El defraudador le comenta que para llevar a cabo ese proceso es necesario que autorice el depósito por medio de su número de cliente y contraseña, el defraudador solicita ambos datos mientras se conecta a la sesión bancaria del cliente.

Fase 3: Alta de cuenta para tercera persona.

Una vez iniciada la sesión en línea en el portal bancario del cliente, el defraudador revisa los saldos de las cuentas y valida cuánto puede obtener; así mismo, genera un alta de tercero en el portal (cuenta del mismo defraudador) y programa una transferencia por el monto validado previamente.

El defraudador, le informa al cliente que la autorización está lista y que debe esperar un determinado tiempo para entrar a su sesión bancaria y validar el supuesto depósito, mientras este tiempo ocurre, la transacción programada se lleva a cabo y las cuentas del cliente quedan vacías, en el momento en el que el cliente entra a revisar, el robo, se ha llevado a cabo.

Acciones después del fraude.

Comunicación y concientización al cliente, es importante mantener una comunicación continua con los clientes, sobre los procesos de seguridad que tiene la institución y pasos de verificación que ellos deben de seguir para evitar caer en fraudes como en el anterior.

La comunicación y concientización se puede realizar de la siguiente manera:

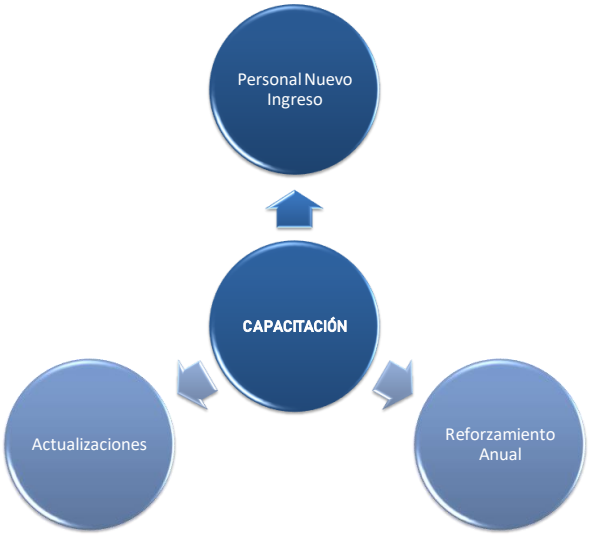
1. Enviando boletines regularmente a los clientes, sobre la importancia de NO compartir por ningún motivo, sus contraseñas, incluso si un supuesto empleado de la institución bancaria se les solicita.
2. Invitar a los clientes a comunicarse a los centros de atención de la institución en caso de percibir o detectar alguna situación extraña en sus cuentas, tarjetas o servicios para recibir asesoría directa de la institución bancaria.
3. Activar sus alertas de movimientos y transacciones en sus celulares y/o correo electrónico, con el fin de que estén enterados de lo que está pasando en tiempo real en sus cuentas.

4.8 Entrenamiento y concientización al personal.

Todos los miembros que forman parte de la institución son responsables de la ejecución, mantenimiento, y mejoras de los controles contra el fraude. Como hemos visto los empleados son la mejor arma contra el fraude, así como también son una fuente valiosa de información, por ello es importante que las instituciones generen y proporcionen constantemente capacitaciones anti-fraude para todos los empleados sin importar el nivel. El entrenamiento constante ayuda a mantener a los empleados bien informados, de esta manera ellos podrán identificar actividades sospechosas y la manera correcta de actuar para combatirlo y/o prevenirlo.

El entrenamiento y/o capacitación debe de contener información clara y objetiva de tal manera que se facilite a los empleados la compresión de la misma; es importante no saturarlos con tanta teoría y palabras técnicas ya que pueden hacerlo tedioso y llegar a confundir a los empleados, una manera en la cual se puede evitar esos conflictos, es mediante el planteamiento de casos prácticos que permitan a los empleados comprender el cómo se llevan a cabo los fraudes y la manera correcta en la que deben de actuar.

La capacitación debe de proporcionarse en los siguientes escenarios:



a) Cuando un nuevo empleado se incorporé a la institución es recomendable que se le proporcione las capacitaciones pertinentes contra el fraude y el reto de las estrategias de control, de esta manera se involucrará con la cultura de la institución y las acciones a seguir en caso de que tenga sospecha de una situación de fraude.

b) Es recomendable que la institución realice un reforzamiento de manera anual a todos los empleados, de esta manera se asegurará de fortalecer los conocimientos y acciones que deben de realizar contra el fraude.

c) En caso de que se realicen cambios a políticas internas o por parte de los reguladores, es necesario que se realicen los reemplazos o modificaciones pertinentes en las capacitaciones proporcionadas al personal, con el objetivo que los empleados cuenten con la información actualizada.

Anteriormente el material de capacitación se proporcionaba por medio de impresiones en papel; las cuales afectaban el medio ambiente y en ocasiones la documentación era archivada o destruida por los empleados sin ser vistas; en la actualidad el método más común es la utilización de las herramientas informáticas, por ejemplo, por medio de boletines, tutoriales, presentaciones cargadas y presentadas en las redes internas de la institución, por medio de correos electrónicos, etc.

Estas herramientas son de gran utilidad para las instituciones ya que permiten que los empleados se programen y/u organicen su tiempo de acuerdo a su horario laboral, es importante indicar alguna fecha limite en la cual deben concluirlas, de lo contrario este tipo de información podría tomarse a la ligera posponiéndola continuamente.

También es de gran utilidad para aquellas instituciones que cuentan con una extensa plantilla de personal, sin embargo, no perdamos de vista que puede que algunos

empleados solo avancen la hoja sin leer detenidamente o comprender la información, para ello la institución se puede apoyar en dos acciones:

1. Evaluaciones, al momento que el empleado finalice la lectura del material proporcionado, deberá responder un cuestionario enfocado al tema en cuestión, manejando un parámetro de aprobación, es decir, cumplir con un rango de aciertos, así podrá asegurarse que el empleado comprendió correctamente, las situaciones de riesgo que pueden presentarse y las acciones a efectuar.
2. Realizar entrenamientos presenciales, el oficial de fraude con el apoyo del área de control y cada uno de los representantes de departamentos pueden organizar sesiones en grupos, para llevar a cabo un reforzamiento de la capacitación de manera más personal, ya que de esta manera permite a los empleados participar activamente, discutir algunas dudas o riesgos que ellos identifican, interactuar entre sí, etc.

Además de proporcionales las capacitaciones necesarias, la institución debe lograr concientizar a los empleados, que tomen el compromiso de defender su trabajo y la institución en la que están, mediante:

1. Motivación, que los empleados se sientan cómodos con su trabajo, que comprendan el por qué lo hacen y sean reconocidos por su buena ejecución.
2. Inclusión, que el empleado se siente parte de la institución, que es escuchado en sus inquietudes y propuestas de mejoras, que consideren que el beneficio obtenido es para las dos partes.

En la medida en que todos los empleados de la institución tengan claro que tipos de riesgos se presentan día a día, cual es la manera correcta de actuar, estar consientes que las medidas de control se implementan para cuidar su integridad, su trabajo y a la institución; disminuirán significativamente los riesgos contra un ataque de fraude.

Conclusiones.

Debido a que en los últimos años el mercado financiero ha presentado grandes cambios en la competencia, el cambio continuo de las necesidades del cliente, nuevas líneas de negocios, estrategias, nuevos productos, fusiones y avance tecnológico, ha llevado a las instituciones financieras a realizar mejoras y cambios en la manera de operar, así como el cuidado y tratamiento de la información que manejan día a día, ya que grandes cambios y mejoras llevan consigo una amenaza para la misma ya que conlleva cierta complejidad en el tratamiento de la información y ejecución de los procesos que pueden poner en riesgo a la institución ante fraudes, pérdida de información, lavado de dinero, amenazando la estabilidad financiera, reputacional y legal.

Este tipo de riesgos y afectaciones son efectuadas porque no se cuenta con los conocimientos e información adecuada, desatención o falta de implementación de controles internos; por ello la importancia de la aplicación de “Control interno” el cual, como se observó en el desarrollo de la tesis tiene por objetivo elaborar y ejecutar planes de acción, políticas, metodologías, etc., que ayuden a reforzar las debilidades de los procesos, así como saber identificar los riesgos que amenazan a la institución y cuál es la manera correcta de actuar para poder combatirlos y mitigarlos, con la finalidad de resguardar cada uno de los activos de la institución para el cumplimiento de sus objetivos de una manera segura.

Recordemos que el control interno es un elemento tan amplio e importante que puede ser aplicado en todos los departamentos, de acuerdo a sus diversas metodologías para enfrentar riegos de fraude, lavado de dinero, seguridad de la información, cada uno de ellos con sus políticas y procedimientos especiales, la aplicación del control interno permitirá medir las debilidades y fortalezas de cada departamento, procedimientos, empleados, etc. asegurándose de encaminar a cada uno de ellos a una cultura organizacional de seguridad, concientización, responsabilidad, comunicación y la colaboración de cada uno de los empleados que forman parte de ella; recordemos que para tener un sistema de control interno fuerte y eficaz es importante la participación de todas aquellas personas que están involucrados, es decir mantener comunicación con los proveedores, clientes, empleados de todos los niveles, un compromiso en conjunto lleva a una institución fuerte y capaz de combatir cualquier probabilidad de riesgo.

Bibliografía.

Aceituno Canal Vicente / Seguridad de la Información / Creaciones Copyright, España, 2004.

Baxter Keith / Administración del Riesgo / Editorial Trillas, México, 2012.

Cano Jeymi / Inseguridad de la Información una visión estratégica / Editorial Alfaomega,2000.

Estupiñán Gaitán Rodrigo / Administración de Riesgos E.R.M y la Auditoría Interna / Editorial ECOE Ediciones / Segunda edición, Bogotá 2015.

Estupiñán Gaitán Rodrigo / Control interno y fraudes, análisis de informe COSO I,II y III con base en los ciclos transaccionales / Editorial ECOE Ediciones / Tercera edición 2016.

Fonseca Luna Oswaldo / Sistemas de Control Interno para Organizaciones / Editorial IICO / Primera edición, Lima 2011.

Isaza Serrano Alejandro Tadeo / Control interno y sistema de gestión de calidad_ guía para su implantación en empresas públicas y privadas / Ediciones de la U,2014.

Juran J. Juran / Planificación de la calidad / Ediciones Díaz de Santos, España, Reimpresión Madrid 2007.

López Bentacourt Eduardo, Porte Petit Moreno Luis Octavio / El Delito de Fraude (Reflexiones) / Editorial Porrua, México.

Mantilla Samuel Alberto / Control Interno: Informe COSO / Editorial ECOE Ediciones Cuarta Edición, Madrid 2005.

Mota Aragón Beatriz / Teoría y aplicaciones en la administración de riesgos / Editorial MA Porrua, México 2015.

Norma ISO 27001 Sistemas de Gestión la Seguridad de la Información / Versión 2018.

Norma ISO 9001 Sistema de Gestión de Calidad / Versión 2015.

Núñez Mora José Antonio, Chávez Gudiño José Juan / Revista Análisis Económico artículo Riesgo Operativo: esquema de gestión y modelado del riesgo, México 2010.

Perdomo Moreno Abraham / Fundamentos de Control Interno / International Thomson Editores, México 2004.

Pérez Fernández José Antonio / Gestión por procesos como utilizar ISO 9001 2000 / Editorial ESIC, Madrid 2010.

Ponce Rivera Alejandro y Chávez, Evelyna Ponce y Chávez / Discrepancia y lavado de dinero 2005 / Editorial ISEF / Primera edición, México 2005.

Santillana González Juan Ramón / Sistema de Control Interno / Editorial Pearson Tercera Edición,México 2015.

Web Library.

Autoridades PLD sitio web:

https://www.cnbv.gob.mx/PrevencionDeLavadoDeDinero/Documents/Régimen%20Nacional%20Jornada%20PLD.pdf.

Comisión Nacional Bancaria y de Valores / Concepto Lavado de dinero sitio web consultado: https://www.cnbv.gob.mx/PrevencionDeLavadoDeDinero/Documents/VSPP_Lavado%20de%20Dinero%20%20%20130701.pdf

Committee Of Sponsoring Organizations of the Treadway Commission (COSO) – Control Interno sitio web: https://www.aec.es/web/guest/centro-conocimiento/coso

Comité de Supervisión Bancaria de Basilea – Concepto de Riesgo Operativo sitio web consultado:

https://www.bis.org/bcbs/charter_es.pdf

Ley de Instituciones de Crédito sitio web – CBV / Acciones y programas / Normatividad Vigente

https://www.cnbv.gob.mx/Paginas/NORMATIVIDAD.aspx

Programa anti fraude sitio web:

http://www.revistadelfraude.com/julio_agosto_15/articulo_fraude_7_pasos.html

Recomendaciones GAFI sitio web: http://www.pld.hacienda.gob.mx/work/models/PLD/documentos/recomendaciones_gafi.pdf.

Riesgo de fraude sitio web:

https://auditoresinternos.es/uploads/media_items/fábrica-fraude.original.pdf

Seguridad de la información sitio web:

https://prezi.com/x40ezhztcaux/modelo-decisional-de-la-piramide-de-anthony/

Seguridad de la información Russell Ackoff y Daniel Greenberg sitio web:

http://insecurityit.blogspot.com/2010/01/la-seguridad-de-la-informacion-una.html

Villalón Huerta, Antonio / Concepto Seguridad Física sitio web consultado: https://www.rediris.es/cert/doc/unixsec/unixsec.pdf

Triángulo de fraude sitio web: https://fraudeinterno.wordpress.com/2018/04/14/el-triangulo-clasico-del-fraude-de-donald-cressey/