HOTEL HILTON CARTAGENA

JULIO 30 2019

19° CONGRESO PANAMERICANO
DE RIESGO DE LAVADO DE ACTIVOS
Y FINANCIACIÓN DEL TERRORISMO

BALANCE Y RETOS PARA EL CUMPLIMIENTO
DE LOS ESTÁNDARES INTERNACIONALES

IVAN DANILO ORTIZ

Implementación de la Norma ISO 31000 en la administración del riesgo de lavado de activos y el financiamiento del terrorismo

Introducción

EVOLUCION TECNOLOGIA PROVOCA CAMBIOS EN MODELOS

RIESGOS REPUTACIONALES

DISTORSIÓN ECONÓMICA INESTABILIDAD FINANCIERA

EROSIÓN DE NORMAS ÉTICAS COLECTIVAS

ISO 31000 CUBRE ÒPTICA ECONÒMICA, GEOPOLITICA, AMBIENTAL, SOCIAL Y TECNOLÒGICA

FMI DE $ 800 MM A $ 2B. DE DINERO ILÌCITO LAVADO ANUALMENTE 2% - 5% DEL PIB MUNDIAL

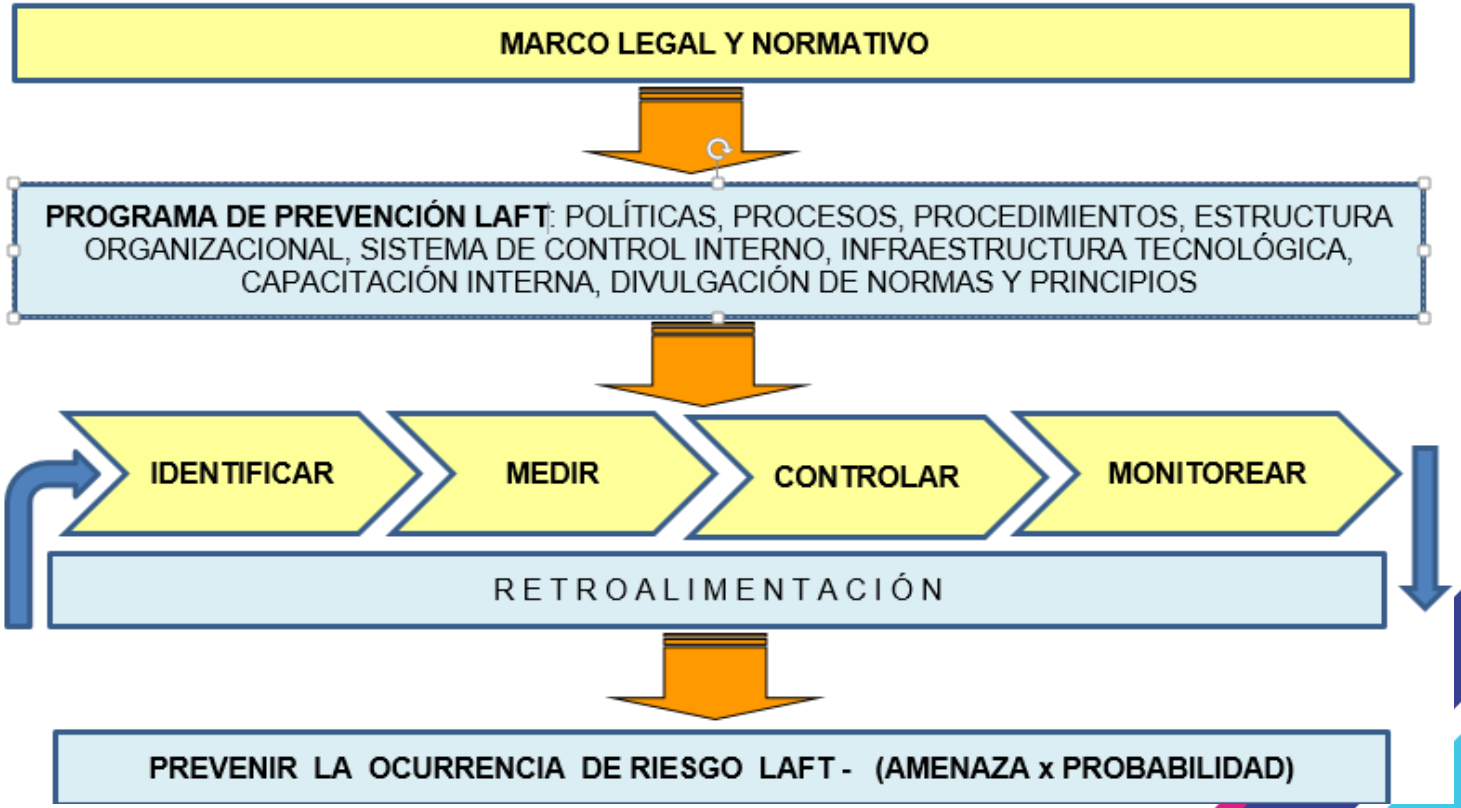
Avance de tecnologías disruptivas

- Regulaciones de Fintech colombianas pronto permitirán usar más tecnología y data en procesos AML ya que el regulador está actualizando sus reglas.
- La SFC proyecta hacer de las licencias para las *startups de fintech* una prioridad y está trabajando en los cambios en el sistema SARLAFT.
- Las nuevas reglas abrirán las puertas a las instituciones financieras para usar más tecnología y data para los análisis background de clientes que necesiten para cumplir con las regulaciones AML.
- KYC más tecnológico, datos sustitutos a la hora de diligenciamiento de ese conocimiento del cliente diferente al tradicional (redes públicas, IA, Data Analytics, bigdta).

Comprensión del entorno tecnológico

- La importancia pragmática de los datos (bigdata).
- Transformación, evolución y aplicación de la banca tradicional a la banca digital.
- Cumplimiento e incertidumbre en cambios normativos.
- Vulnerabilidad de los sistemas de TI (ciberseguridad, nube, multicanal, blockchain, Fintech, IA)
- Afrontar riesgos y amenazas: *mejora toma de decisiones*, plan contingente durante disfunciones, *visión integral* del negocio, *asignación eficiente* de recursos.

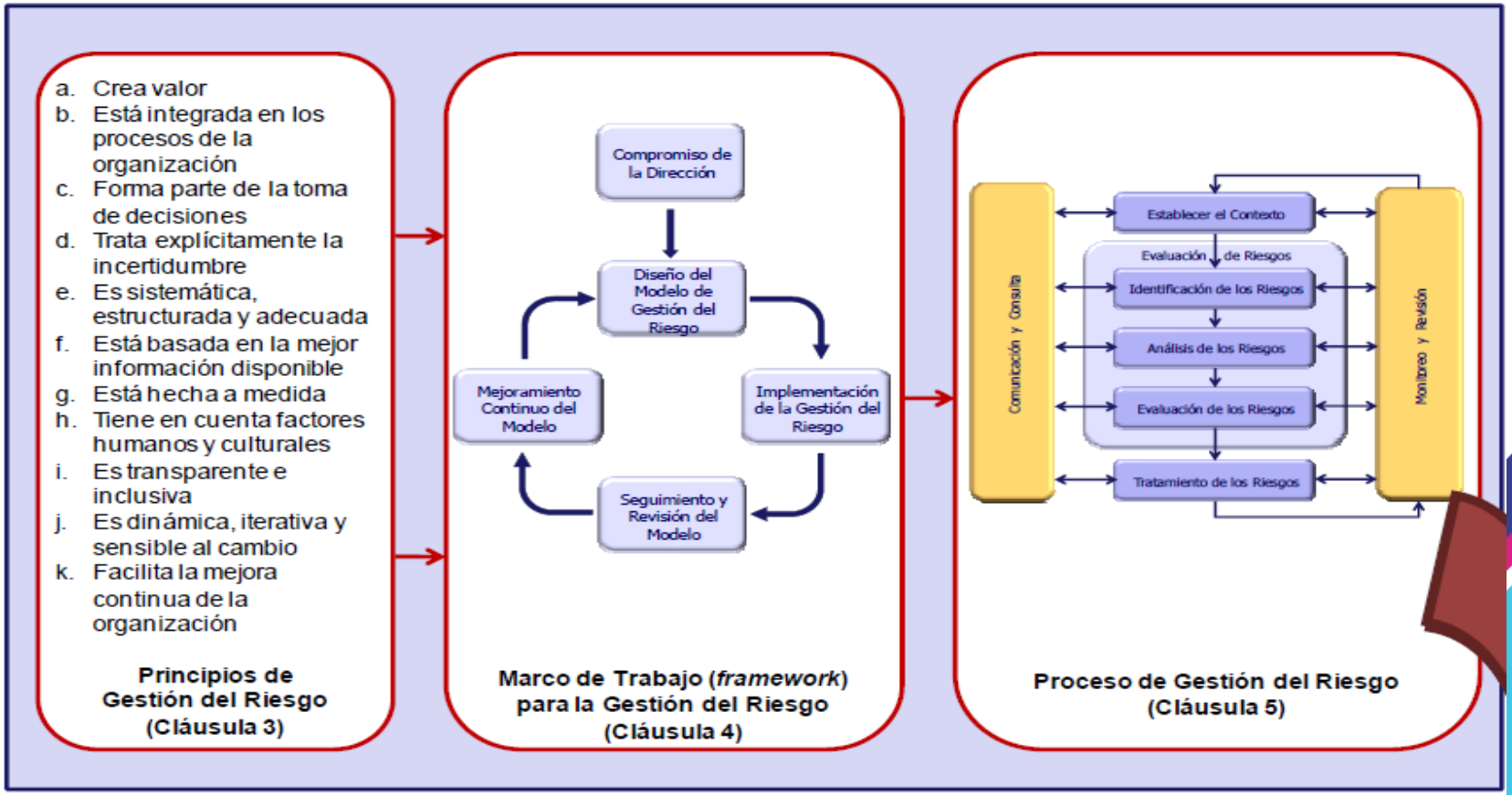
Metodología de administración



ISO 31000 para solventar deficiencias

- Disponer de una calificación individual y monitoreo de clientes con perfil de riesgo demográfico y transaccional.
- Diseñar controles preventivos en función de la identificación del riesgo integral (cualitativo y cuantitativo).
- Establecer *niveles de tolerancia* a los riesgos identificados.
- Cumplir con las disposiciones legales locales e internacionales.
- Acercar, mejorar e integrar las relaciones con las partes interesadas (*Matriz de stakeholders*).
- Ayudar a alcanzar los objetivos estratégicos de las organizaciones, que se reflejan en mayor rentabilidad y crecimiento en el mercado.

ISO 31000 modelo gestión de riesgo



ISO 31000 – Versión 2018

El liderazgo, compromiso e integración de posibles amenazas dentro de la estructura de la empresa

Principios ISO 31000:2009	Proceso de gestión de riesgo	Aplicación práctica de los principios en el modelo de gestión	Principios ISO 31000:2018
1. Crea valor	Establecer el contexto	Contribuye al logro de los objetivos y a la mejora del desempeño	1. Integrado en todas las actividades
2. Está integrada en los procesos de la organización	Todo el proceso de Gestión del Riesgo	Política para la Gestión integral de Riesgos de las Entidades de los Sectores Financieros Público y Privado	
3. Trata explícitamente la incertidumbre	Identificación, Análisis y Evaluación del Riesgo	Control PLAFD en procesos de ingreso o recepción de fondos de clientes y aceptación de un nivel de riesgo	
4. Forma parte de la toma de decisiones	Todo el proceso de Gestión del Riesgo	Ayuda a tomar decisiones o elecciones informadas sobre los niveles tolerables de aceptación del riesgo de LAFD	
5. Es sistemática, estructurada y adecuada		Todo el modelo ISO 31000 funciona como un conjunto, con un orden cronológico y estructurado	2. Estructurado
6. Está basada en la mejor información disponible		Apoyado en la información existente al interior y fuera del banco	3. Basado en la mejor información disponible.
7. Está hecha a medida		La gestión de riesgo está apoyada en un software de monitoreo	4. Adaptado a la organización
8. Tiene en cuenta factores humanos y culturales		Ayuda a identifica la "cultura organizacional" de la entidad bancaria	5. Considera factores humanos y culturales.
9. Es transparente e inclusiva		Participación inclusiva de todos las partes (Matriz de stakeholders)	6. Inclusivo de todas las partes interesadas
10. Es dinámica, interactiva y sensible al cambio	Establecer el contexto	Modelo flexible y dinámica en su enfoque de gestión	7. Dinámico y con respuesta a cambios
11. Facilita la mejora continua de la organización	Marco de trabajo	Bases para diseñar, controlar y realizar la mejora continua	8. Enfocado a la mejora continua

CREAR Y MANTENER VALOR

Marco de trabajo – gestión de riesgo

Compromiso de la Dirección

Diseño del Modelo de Gestión de Riesgo

- Comprensión de la organización y su contexto
- Establecimiento de política de gestión de riesgos
- Rendición de cuentas
- Integración de procesos de la organización
- Recursos
- Establecimiento de mecanismos de comunicación interna y reporte
- Establecimiento de mecanismos de comunicación externa y reporte

Implementación de la gestión del Riesgo

Seguimiento y Revisión del Modelo

Mejoramiento continuo del modelo

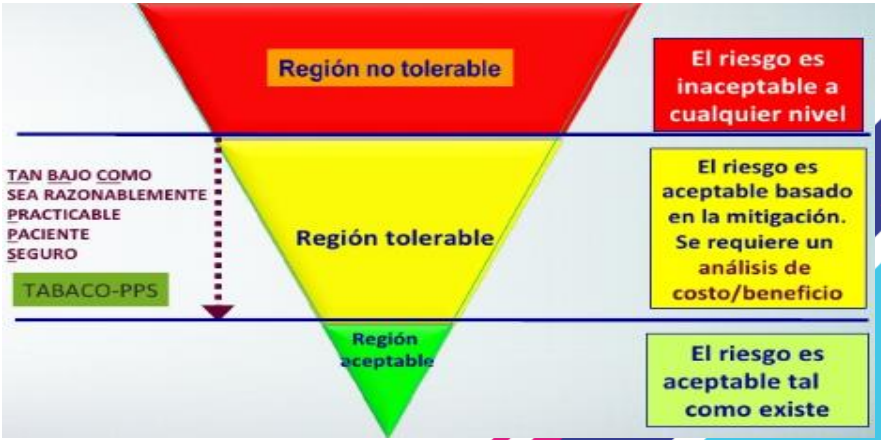
I. Comunicación y consulta

Compliance Officer: rol de enlace con actores internos y externos que interactúan en la Gestión del Riesgo, que debe acoplarse con otras áreas y funciones de la organización, que considere:

- Fuente de valor agregado para la entidad (*alinear a objetivos*)
- Incorporar varios puntos de vista (*consenso de criterios*)
- Promover un ambiente de confianza (*prácticas colaborativas*)
- Optimizar la evaluación de riesgos (*matriz de actores*)

II. Establecer el contexto

- Implementar un SGR integral que incluya *impacto* de las *tecnologías disruptivas* que evite que los servicios financieros sean utilizados para actividades ilícitas.
- Identificación y análisis de las partes (stakeholders) bajo enfoque de LAFT.
- Criterios de determinación y medición de los niveles de riesgo
  - (1) Riesgo Bajo
  - (2) Riesgo Medio
  - (3) Riesgo Alto
  - (4) Riesgo Extremo



III. Identificación del riesgo

El propósito es generar una lista de fuentes de riesgos y eventos de LAFT que pueden tener un alto impacto.

Según el cliente
a.- Tipo de cliente
b.- Nacionalidad
c.- Actividad económica
d.- Sub-segmento de negocio
e.- Edad del cliente / antigüedad
f.. Agencia de anclaje (zona geográfica)
g.- Ingreso persona natural / jurídica
h.- Patrimonio persona natural / jurídica
i.- Domicilio del cliente
j.- Género

Según las operaciones
a.- Propósito de la cuenta
b.- Fuente u origen de fondos
c.- Frecuencia de ingresos
d.- Antigüedad de la cuenta
e.- Canales transaccionales
f.- Productos y servicios
g.- Tipo de transacción

IV. Análisis del Riesgo - Clientes

Clasificación de riesgo por rango de edad y antigüedad

Tipo de cliente	Rango de edad y/o antigüedad	Riesgo
Persona natural	1 - 25 años	Extremo
	26 - 35 años	Alto
	36 - 65 años	Medio
	Mayor a 65 años	Bajo
Persona jurídica	1 día - 6 meses	Extremo
	7 meses - 12 meses	Alto
	13 meses - 36 meses	Medio
	Más de 37 meses	Bajo

Clasificación de riesgo por ingresos de clientes

Tipo de cliente	Rango de ingresos US $	Riesgo
Persona natural	1 - 520	Bajo
	521 - 1.800	Medio
	1.801 - 20.000	Alto
	Mayor a 20.001	Extremo
Persona jurídica	0 - 850.000	Extremo
	850.001 - 3.400.000	Alto
	3.400.001 - 5.900.000	Medio
	Mayor a 5.900.001	Bajo

IV. Análisis del Riesgo - Operaciones

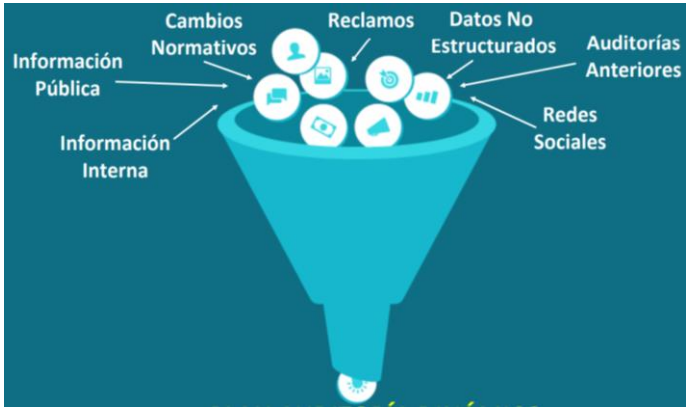
Detalle de canales de servicios bancarios

Canales	Detalle del canal	Riesgo
FÍSICO	Agencias	Alto
	Ventanilla de atención	Alto
	Puntos pago	Medio
	Ventanilla Express	Bajo
	Corresponsal no bancario (CNB)	Bajo
INTERNET	Banca electrónica personas (banca digital)	Extremo
	Banca electrónica empresas (cash management)	Extremo
AUTOSERVICIO	Kioscos de consultas y transacciones	Alto
	Cajeros automáticos	Medio
	Depositarios	Medio
CELULAR	Servicio telefónico transaccional en agencia	Bajo
	Celular	Alto
	Dispositivos móviles (tecnologìas disruptivas)	Extremo
TELEFÓNICO	IVR (Interactive Response Unit) reconocimiento de voz	Medio
	Call center	Medio
	Telemercadeo	Bajo

V. Evaluación del Riesgo - Cualitativo

Se utiliza información que tiene *relación* con cada uno de los componentes que forman parte de los factores de riesgo:

- Artículos de prensa internos y externos
- Análisis y estudios, señales de alerta, tipologías de la UAF, GAFI, GAFILAT, EGMONT, ONU, FMI, BM.
- Impacto de las tecnologías disruptivas en la valoración y aceptación del riesgo.
- Informes de casos relacionados con prevención de LAFT.
- Información histórica relevante de la entidad o sector económico.



V. Evaluación del Riesgo - Cuantitativo

Cada factor forma parte de la matriz de riesgo, que una vez *consolidados permiten establecer un nivel de riesgo ponderado* que facilita la comparación con los niveles de riesgo definidos en el establecimiento del contexto, en función del software AML que posea cada banco.

Rangos para la calificación de riesgos

Rangos	Riesgo
1,0 - 2,0	BAJO
2,1 - 3,0	MEDIO
3,1 - 4,0	ALTO
4,1 - 5,0	EXTREMO

Rangos	Riesgo
0 - 1,0	BAJO
1,1 - 2,0	MEDIO
2,1 - 3,0	ALTO
3,1 - 4,0	EXTREMO

Rangos	Riesgo
0 - 65	BAJO
66 - 85	MEDIO
86 -89	ALTO
90 - 100	EXTREMO

Consolidación - Matriz de Riesgos

El resultado es producto de la combinación de 2 funciones tanto de las condiciones de vulnerabilidad y las condiciones de amenaza, que en el caso son de 1,38 y 4,47 respectivamente.

MATRIZ RIESGO DE CLIENTE

Condiciones de Vulnerabilidad			
Factor	**Ponderaciòn**	**Riesgo**	**Puntaje**
Edad del cliente	6%	3	0,18
Agencia de anclaje	10%	3	0,3
(a) Subtotal	16%		**0,48**
Condiciones de Amenaza			
Tipo de cliente	5%	3	0,15
Nacionalidad	5%	2	0,1
Actividad econòmica	15%	4	0,6
Subsegmento de negoci	15%	3	0,45
Ingreso promedio	10%	1	0,1
Patrimonio	15%	1	0,15
Domicilio del cliente	14%	3	0,42
Gènero	5%	3	0,15
(b) Subtotal	84%		**2,12**
Total Factor Cliente	**100%**		2,6

MATRIZ RIESGO DE OPERACIONES

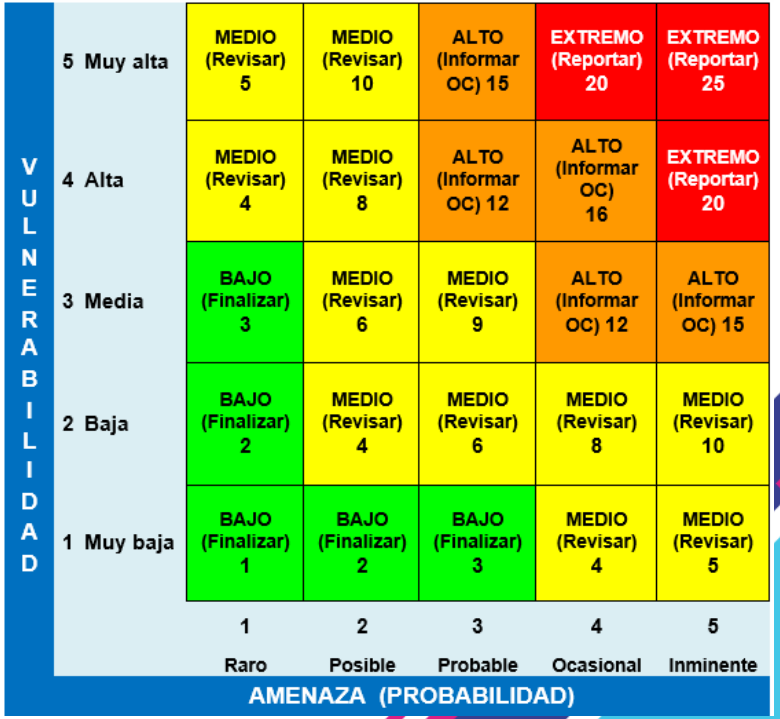
Condiciones de vulnerabilidad			
Factor	**Ponderaciòn**	**Riesgo**	**Puntaje**
Propòsito de la cuenta	5%	3	0,15
Productos o servicios	25%	3	0,75
(a) Subtotal	30%		**0,9**
Condiciones de Amenaza			
Fuente u origen de fondos	5%	3	0,15
Ciclo de ingresos	5%	3	0,15
Antiguedad de la cuenta	10%	1	0,1
Canal transaccional	5%	3	0,15
Tipo de transacciòn	45%	4	1,8
(b) Subtotal	70%		**2,35**
Total Factor Operaciones	100%		3,25
RESULTADO COMBINADO (∑a + ∑b)			**1,38 - 4,47**

Riesgo inherente – Vulnerabilidad x Amenaza

Los resultados de la matriz de riesgo sirven de base para la ejecución del *monitoreo*, adoptando las *medidas de debida diligencia* que corresponda.

Calificación de riesgos

Vulnerabilidad	Amenaza	Resultado	Calificación	Acción
1	1	11	RIESGO BAJO	Finalizar
1	2	12	RIESGO BAJO	Finalizar
1	3	13	RIESGO BAJO	Finalizar
1	4	14	RIESGO MEDIO	Revisar
1	5	15	RIESGO MEDIO	Revisar
2	1	21	RIESGO BAJO	Finalizar
2	2	22	RIESGO MEDIO	Revisar
2	3	23	RIESGO MEDIO	Revisar
2	4	24	RIESGO MEDIO	Revisar
2	5	25	RIESGO MEDIO	Revisar
3	1	31	RIESGO BAJO	Finalizar
3	2	32	RIESGO MEDIO	Revisar
3	3	33	RIESGO MEDIO	Revisar
3	4	34	RIESGO ALTO	Informar al OC
3	5	35	RIESGO ALTO	Informar al OC
4	1	41	RIESGO MEDIO	Revisar
4	2	42	RIESGO MEDIO	Revisar
4	3	43	RIESGO ALTO	Informar al OC
4	4	44	RIESGO ALTO	Informar al OC
4	5	45	RIESGO EXTREMO	Reportar Comité
5	1	51	RIESGO MEDIO	Revisar
5	2	52	RIESGO MEDIO	Revisar
5	3	53	RIESGO ALTO	Informar al OC
5	4	54	RIESGO EXTREMO	Reportar Comité
5	5	55	RIESGO EXTREMO	Reportar Comité



Riesgo residual

- Efectividad control sobre tecnologías disruptivas
- Falla de control incremento del riesgo residual

Riesgo Inherente	(-)	Valor del Control	=	Riesgo Residual

Expectativa
- Efectividad del control
- Promesa

Control sub-estándar	=	- 1	Falla el control, no funciona
Control original	=	0	Con los controles actuales
Control reforzado	=	+ 1	Aumenta expectativa
Control adicional	=	+ 2	Refuerza expectativa

FINCEN MULTA A UN CAMBISTA CRIPTOGRÁFICO P2P POR COMPRAR, VENDER MILLONES DE DÓLARES EN BITCOIN Y NO PRESENTAR INFORMES

VI. Tratamiento del Riesgo

En función de *formular las estrategias* para establecer los controles necesarios sobre la base del *grado de exposición* y *nivel de aceptación* del riesgo.

Alternativas de estrategias de gestión del riesgo

EVITAR	Se evita el riesgo cuando se decide no comenzar o no continuar con la actividad que da origen a este
PREVENIR	Implica actuar sobre los factores de riesgo antes que se concrete un evento inusual e injustificado con indicios de LAFD
PROTEGER	Proteger el riesgo con el propósito de limitar las consecuencias que se pueden derivar de su materialización
ACEPTAR	Implica asumir el riesgo en las condiciones en el que éste se encuentra sin desarrollar medidas o acciones adicionales

VII. Monitorear y revisar

- Los procesos de gestión de riesgos deben ser *incorporados a procesos organizacionales* y al plan estratégico de la entidad.
- Puede ser ejecutado con el apoyo de *indicadores de gestión* y umbrales de control, a cargo de Riesgos, Cumplimiento, Operaciones, Auditoría interna, BI.
- Indicadores: *medibles*, tener una *definición*, un *alcance*, y un *responsable* a cargo de esta medición periódica.
- Indicador permite realizar acciones de ajuste al sistema que facilita la adopción de correcciones oportunas frente a las desviaciones.

Identificar métricas relevantes que provean datos útiles sobre potenciales riesgos que impactan el logro de los objetivos

VII. Monitorear – Indicadores KCI

- Conocer objetivos y riesgos
- Modelo y plan de negocio
- Mapeo de riesgos que impacta
- Métricas del indicador de riesgo
- Documentar el indicador

VII. Monitorear - Indicador ROS

Concepto	Descripción
PROCESO	MONITOREO DE TRANSACCIONES DE CLIENTES
SUBPROCESO	Reportes de operaciones inusuales e injustificadas (ROII) remitidos a la UAFE
DEFINICION	Representa el nivel de operaciones inusuales realizadas por los clientes en la entidad identificadas en el monitoreo, sin justificación y reportadas a la UAFE
MEDICION	Mensual
META	Lograr identificar, gestionar y evaluar las transacciones que exceden el perfil de riesgo asignado al cliente, para someterlas a un proceso de revisión y debida diligencia para justificar la excepción alertada por el sistema de monitoreo y que NO fueron justificadas por el cliente
VERIFICAR	Realizar el seguimiento que todas las operaciones inusuales alertadas sean gestionadas con apoyo del Ejecutivo de Cuenta y que exista una respuesta del cliente, y reportar a la UAFE aquellos casos que no fueron justificadas por el cliente
FORMA DE CALCULO	Número de ROII de clientes reportados a la UAFE / Número de alertas gestionadas con el Negocio para descarte x 100
	Número. de alertas gestionadas con el Negocio para descarte / Número total de clientes alertados por sistema de monitoreo x 100
RESPONSABLE	Unidad de Cumplimiento / Ejecutivos de Negocio
FINALIDAD	Mide el nivel porcentual de las transacciones inusuales e injustificadas reportadas a la UAFE con relación al total de transacciones alertadas y gestionadas con el Negocio para descarte
FUENTE DE INFORMACION	Base de datos del software de monitoreo, tanto de los casos alertados de transacciones inusuales, como los casos injustificados y reportados a la UAFE
NIVEL DE REPORTE	Comité de Cumplimiento y Comité Integral de Riesgos
FUENTE DEL INDICADOR	Indicador requerido por la Superintendencia de Bancos y Comité de Riesgos

Conclusiones

- ISO 31000 persigue disminuir probabilidad de impactos de eventos de LAFT y busca generar más negocios seguros.
- El conocimiento y *enfoque integral del riesgo*, permite a las IFIS realizar una *planificación estratégica más efectiva*.
- El éxito del sistema, es el *compromiso de la alta gerencia* para apoyar la eficaz y eficiente ejecución del programa AML.
- El compromiso que se genera al involucrar a las partes interesadas, ayuda a *alinear los esfuerzos de la gestión de riesgos a los objetivos estratégicos* de la organización.
- La revolución digital es un hecho económico y cultural, abre oportunidad de ampliar el mercado con base a una adecuada Gestión Integral de Riesgo.

Dr. Iván Danilo Ortiz, CPA, AML/CA

dusnavy@gmail.com / ortizi@fiscalia.gob.ec

(593-2) 2428617 / (593)998021627

Quito, Ecuador