XXIII Congreso Latinoamericano
de Auditoría Interna y Evaluación de Riesgos
Santa Cruz, Bolivia

CLAIN 2019
MAYO
16 Y 17

ASOBAN
ASOCIACIÓN DE BANCOS PRIVADOS DE BOLIVIA

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

"El enfoque de la auditoría interna ante la revolución digital y las innovaciones disruptivas"

XXIII Congreso Latinoamericano de Auditoría Interna y Evaluación de Riesgos
Santa Cruz, Bolivia

CLAIN 2019
MAYO
16 Y 17

ASOBAN
ASOCIACIÓN DE BANCOS PRIVADOS DE BOLIVIA

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

El Rol de la Auditoría Interna en el mundo VICA (Volátil, Incierto, Complejo, Ambiguo)

Dr. Iván Danilo Ortiz

ECUADOR

Panorama del Entorno

EVOLUCION TECNOLOGIA PROVOCA CAMBIOS EN MODELOS DE NEGOCIOS

RIESGOS REPUTACIONALES

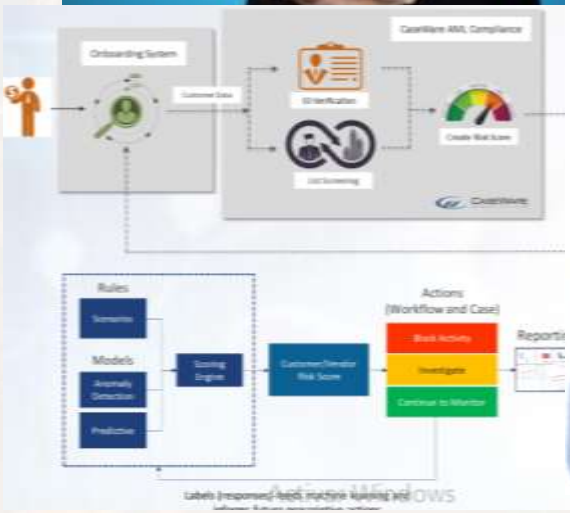
EROSIÓN DE NORMAS ÉTICAS COLECTIVAS

Introducción

- Evolución disruptiva de medios tecnológicos provoca cambios en modelos de negocio, que obligan a la evolución de la *"Administración de Gestión de Riesgos"*.
- Las regulaciones de Fintech pronto permitirán usar más tecnología y data en procesos.
- Las normas de control alientan el uso de información y datos personales aprovechando la tecnología.
- Auditoría interna debe ajustar el enfoque de revisión de acuerdo al avance tecnológico y tendencias disruptivas.

I. Comprensión del entorno tecnológico

- La importancia pragmática de los datos (bigdata, minería: perfiles) aprovecha tecnología.
- Transformación, evolución y aplicación de la auditoría interna digital.
- Cumplimiento e incertidumbre en cambios normativos.



II. Vulnerabilidad de los sistemas de TI

- Afrontar riesgos- amenazas: mejora toma de decisiones, visión integral del negocio, asignación eficiente de recursos.
- Preparación para la ciberseguridad: evaluar entorno respecto a los riesgos.
- Utilización e ingreso a plataformas en la nube, plantea riesgos: pérdida de data, interrupciones y acceso inadecuado a data
- Políticas de uso de cuentas de usuarios y protocolos de seguridad de aplicaciones.

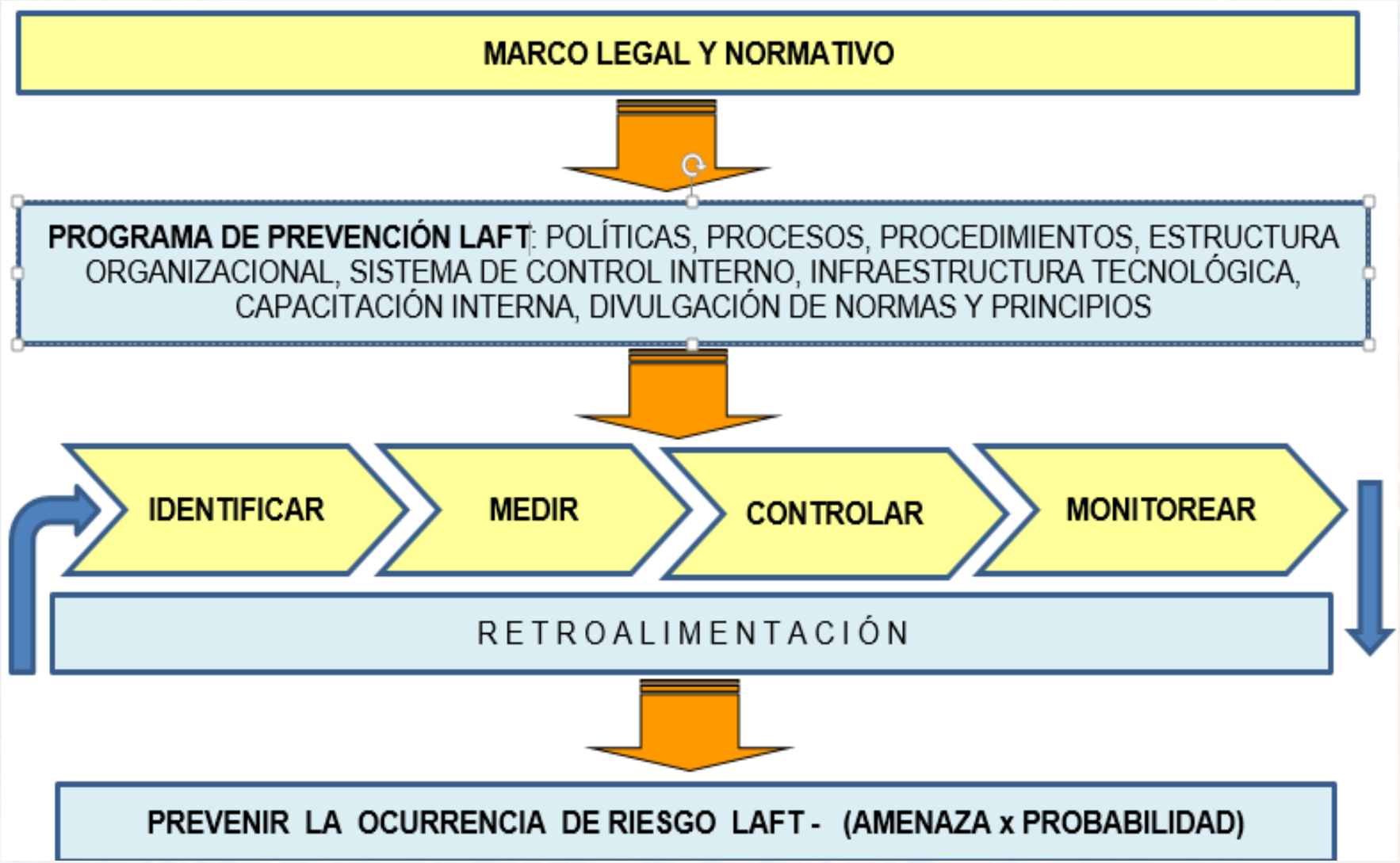
III. Prevención de brechas de seguridad

- Evaluar Plan Seguridad de Datos
- Actualización de políticas de privacidad datos
- Auditoría anual sobre la seguridad de información
- Entrenamiento del personal sobre seguridad datos
- Actualizar inventario de aplicaciones tecnológicas
- Políticas de restricción de dispositivos externos
- Blockchain y encriptación de información sensible

IV. Crecimiento y participación de mercado

- Planificación estratégica e integridad de los empleados, KYE
- Proveedores externos y terceros, para acelerar transformación digital, acceso a plataforma.
- El fenómeno de-risking (El riesgo del no riesgo). Bases técnicas de restricción, alinear objetivos.

V. Riesgo AML/FT desde auditoría interna



V. Consolidación – Matriz Riesgo

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**

V. 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

VULNERABILIDAD	1	2	3	4	5
5 Muy alta	MEDIO (Revisar) 5	MEDIO (Revisar) 10	ALTO (Informar OC) 15	EXTREMO (Reportar) 20	EXTREMO (Reportar) 25
4 Alta	MEDIO (Revisar) 4	MEDIO (Revisar) 8	ALTO (Informar OC) 12	ALTO (Informar OC) 16	EXTREMO (Reportar) 20
3 Media	BAJO (Finalizar) 3	MEDIO (Revisar) 6	MEDIO (Revisar) 9	ALTO (Informar OC) 12	ALTO (Informar OC) 15
2 Baja	BAJO (Finalizar) 2	MEDIO (Revisar) 4	MEDIO (Revisar) 6	MEDIO (Revisar) 8	MEDIO (Revisar) 10
1 Muy baja	BAJO (Finalizar) 1	BAJO (Finalizar) 2	BAJO (Finalizar) 3	MEDIO (Revisar) 4	MEDIO (Revisar) 5
	1 Raro	2 Posible	3 Probable	4 Ocasional	5 Inminente

AMENAZA (PROBABILIDAD)

V. 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

V. 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

VI. Monitoreo continuo de controles

- Nivel de confianza del control interno en contexto de los riesgos.
- Áreas críticas = Evaluación del SCI y las condiciones del entorno.
- Calificación de riesgos (BMAE) y criterios de tolerancia.
- Avances tecnológicos para tratar el riesgo (software o IA).

VI. Monitoreo continuo de controles

PROGRAMA DE CONTROL OPERATIVO DE OFICINAS Y AGENCIAS				VULNERABILIDAD				
				MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
1	RARO	1% – 19%	Podría ocurrir en circunstancias excepcionales. No se conoce incidente alguno en el que el segmento al que pertenece la oficina evaluada haya reportado debilidades de control interno o eventos relacionados a fraudes o transacciones inusuales.	ACEPTABLE	ACEPTABLE	TOLERABLE	TOLERABLE	TOLERABLE
				Control aleatorio según plan de revisión	Control aleatorio según plan de revisión	Control anual general según plan de visitas	Control anual general según plan de visitas	Control anual general según plan de visitas
2	POSIBLE	20% – 39%	Se estima poco factible que ocurra en las circunstancias actuales. La oficina evaluada pertenece a un segmento que no ha reportado incidentes o novedades en las visitas de auditoría en el último año.	ACEPTABLE	TOLERABLE	TOLERABLE	TOLERABLE	TOLERABLE
				Control aleatorio según plan de revisión	Control anual general según plan de visitas	Control anual general según plan de visitas	Control semestral general	Control semestral general
3	PROBABLE	40% – 59%	Resultaría razonable que ocurra. Se estima que podría ocurrir algunas veces en las condiciones actuales en las que se opera. La oficina evaluada pertenece a un segmento que ha reportado al menos un incidente de irregularidad operativa, fraudes o transacciones inusuales en el último año	ACEPTABLE	TOLERABLE	TOLERABLE	INACEPTABLE	INACEPTABLE
				Control aleatorio según plan de revisión	Control anual general según plan de visitas	Control semestral general	Control trimestral detallado coforme plan	Control trimestral detallado conforme plan
4	OCASIONAL	60% – 79%	Existe una probabilidad mayor de ocurrencia. Se estima que podría ocurrir algunas veces en las condiciones actuales en las que se opera. La oficina evaluada pertenece a un segmento que ha reportado más de uno y menos de cinco incidentes en el último año.	TOLERABLE	TOLERABLE	INACEPTABLE	INACEPTABLE	INADMISIBLE
				Control anual general según plan de visitas	Control semestral general	Control trimestral detallado conforme plan	Control trimestral detallado conforme plan	Control bimensual intenso, pruebas de detalle
5	INMINENTE	80% – 100%	Se esperaría que ocurriera en la mayoría de circunstancias. La oficina evaluada pertenece a un segmento que ha reportado más de cinco incidentes en el último año, por lo general son oficinas marcadas como de alto riesgo ya sea por su zona geográfica, tipo de clientes, según los factores de riesgos definidos.	TOLERABLE	TOLERABLE	INACEPTABLE	INADMISIBLE	INADMISIBLE
				Control anual general según plan de visitas	Control semestral general	Control trimestral detallado conforme plan	Control bimensual intenso, pruebas de detalle	Control bimensual intenso, pruebas de detalle

MONITOREO CONTINUO CON CONTROLES PREVENTIVOS Y ALERTAS AUTOAMATIZADAS PARA AUDITORIA INTERNA

VII. Revisión de gestión Gobierno Corporativo

Gobierno Corporativo

- Clientes
- Inversores
- Empleados
- Proveedores
- Comunidad
- Competidores
- Medios
- Regulador

GESTION CONSEJO ADMINISTRACION

- Aprobación objetivos estratégicos
- Miembros del Consejo calificados
- Prácticas de GC acorde a su realidad
- GC en todo el grupo económico
- Actividades acorde a tolerancia, políticas

SISTEMAS DE CONTROL Y EVALUACIÒN

- Función GIR con autoridad, independencia
- Riesgos identificados y monitoreados
- Comunicación interna fluida y oportuna
- Utilizar el trabajo de auditoría interna
- Supervisar sistema de compensaciones
- Compensación alineada a riesgos prudentes
- Conocer estructura operacional y riesgo
- Operar con jurisdicciones de riesgo
- GC transparente frente a los stakeholders

VIII. Planificación bajo incertidumbre

- Cumplimiento normativo, incertidumbre y cambios regulatorios (fintech, regtech, derisking, bigtech) en aumento.
- Incremento de fraudes internos y externos (auditoría forense: prueba legal material).
- Desafíos de implementar las nuevas tecnologías: mejoras internas previas.

Conclusiones

- Auditoría digital innovadora y ágil para crear, mejorar y proteger el valor.
- Nuevas barreras de protección legal y tecnológica que interactúan con los controles internos.
- El compromiso que se genera al involucrar a las partes, *alinea esfuerzos* de la *gestión de riesgos* a *objetivos estratégicos*.
- Desafío: pasar de la banca tradicional a la digital, los esfuerzos de auditoría deben ir dirigidos en ese sentido.

Dr. Iván Danilo Ortiz, CPA, AML/CA

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

(593-2) 2428617 / (593)998021627

Quito, Ecuador