# Las lecciones que nos deja el año 2020: Algunas reflexiones en el Día Nacional de la Prevención del Lavado de Activos

***Juan Pablo Rodríguez C.**
****René M. Castro V.**
*****Camilo A. Rueda B.**

Este 29 de octubre de 2020 se celebra en Colombia y en otros países del mundo el Día Nacional de la Prevención del Lavado de Activos[1] y que mejor ocasión para hacer algunas reflexiones de lo que nos deja este año tan atípico, en el que hemos tenido tantas noticias acerca de este riesgo, empezando por las restricciones debido a la pandemia[2], los FinCEN Files Leaks[3] y la publicación del Índice AML de 2020 de Basilea[4], asuntos sobre los que hemos escrito varios artículos.

Sin embargo, antes de presentar las lecciones que nos han dejado el año 2020, nos queremos referir al Reporte de Costo del Compliance de 2020[5], según el cual, desde el punto de vista de la tecnología, los encuestados pensaron que el mayor cambio para el cumplimiento en los próximos 10 años sería la automatización de las actividades de cumplimiento. En el primer trimestre de 2020, se publicó su cuarto informe anual sobre fintech, regtech y el papel del cumplimiento. El informe concluyó que la industria de servicios financieros tiene mucho que ganar con la implementación efectiva de fintech, regtech e insurtech, pero hay numerosos desafíos qué superar antes de que se puedan obtener los beneficios potenciales.

Los principales desafíos en 2020 descritos se refieren a mantenerse al día con el cambio regulatorio; el presupuesto y asignación de recursos; la protección de datos (privacidad, gobierno interno, GDPR); la incorporación de cambios regulatorios y; la necesidad de inculcar una cultura de cumplimiento.

En el caso de las Juntas Directivas, sus principales desafíos son: equilibrar presupuestos y aumentar los costos de cumplimiento; el volumen de cambio regulatorio; impulsar un cambio cultural demostrable; el incremento de la responsabilidad personal y la implementación e incorporación del cambio regulatorio.

Finalmente las entidades financieras fueron encuestadas para determinar el Global Systemically Important Financial Institutions (G-SIFIs) y se les preguntó sobre los 12 meses siguientes en relación con: el tamaño del equipo de cumplimiento; el presupuesto total del equipo de cumplimiento; una mayor participación en el cumplimiento para la evaluación de soluciones fintech/regtech y; la tercerización de funciones de cumplimiento.

## Pandemia

Una de las situaciones más complicadas que todos los países experimentamos por la pandemia fue el trabajo en casa y lo que eso significó para los controles, la seguridad de la información, la tecnología, la interacción

[1] Ver programación completa de la celebración en: https://www.negociosresponsablesyseguros.com/agenda-2020/
[2] Ver articulo completo en: https://ricsmanagement.com/press/la-pandemia-y-el-plan-de-continuidad-del-negocio/
[3] Ver articulo completo en: https://ricsmanagement.com/press/fincen-files-leaks-del-dano-publico-a-la-defensa-privada-aspectos-juridicos-y-practicos/
[4] Ver articulo completo en: https://ricsmanagement.com/press/estamos-perdiendo-la-guerra-en-la-lucha-contra-el-lavado-de-activos-y-la-financiacion-del-terrorismo-una-revision-al-indice-amlcft-de-basilea/
[5] Ver en: http://financial-risk-solutions.thomsonreuters.info/Cost-of-Compliance-2020

entre los empleados y la Alta Dirección. Eso fue aún más complicado para las áreas de cumplimiento y control, que si ya antes de la pandemia tenían problemas para interactuar, negociar y conciliar con las diferentes áreas (sobre todo con las áreas comerciales), ahora que no se pueden tener reuniones presenciales, es más difícil obtener aprobaciones de la Alta Gerencia o discutir abiertamente asuntos delicados del Área de Cumplimiento.

Adicionalmente, las empresas debieron adaptar sus procesos internos de gestión de riesgos, cumplimiento y antilavado de dinero (AML) a un entorno de trabajo desde casa.

Igualmente, la implementación de estrategias de teletrabajo utilizando redes privadas virtuales (VPN), servicios de conferencias virtuales y otras tecnologías de telecomunicaciones remotas puede aumentar las vulnerabilidades de la ciberseguridad.

Las empresas enfrentan las mismas preocupaciones que antes, aunque la pandemia las ha intensificado. Las presiones presupuestales por la disminución de los ingresos, la priorización de riesgos, unas actividades altamente reguladas y el cambio de las transacciones presenciales a las transacciones digitales son simplemente la nueva normalidad.

La pandemia hizo evidente la falta de cultura de cumplimiento por parte de los sujetos obligados al no demostrar la cultura y el nivel de cooperación que esperan las autoridades regulatorias, así como la falta de claridad con respecto a los roles y responsabilidades dentro del negocio y el cumplimiento.

Muchas de las políticas y procedimientos no estaban actualizadas con los desarrollos regulatorios ni tampoco se había realizado un análisis de la brecha entre los requisitos reglamentarios y la implementación del sistema ALA/CFT dentro de las empresas y, en cuanto a la metodología de evaluación de riesgos, no se tuvieron en cuenta los productos y servicios de alto riesgo generados por la pandemia.

Los desafíos causados por el COVID-19 han hecho que se eludan o flexibilicen los controles antilavado de dinero o contra la financiación del terrorismo (ALD/CTF), esto incluye desde desafíos de monitoreo de transacciones a nivel bancario hasta menos supervisión y reforma de las políticas ALD/CTF a nivel gubernamental, que a su vez generan fallas en las evaluaciones de controles.

La pandemia ha cambiado hasta la forma tradicional de lavar dinero. Los delincuentes ya se están aprovechando de la pandemia del COVID-19 para llevar a cabo esquemas distintos y explotación a través de una variedad de métodos que incluye desde nuevas formas de ciberdelito, tráfico de medicamentos falsificados, recaudación de fondos para organizaciones benéficas falsas, así como el auge del comercio electrónico que se ha prestado para nuevos delitos, entre otras conductas. Y en este contexto es muy probable que quienes buscan lavar el producto del delito o financiar el terrorismo también aprovechen las debilidades de los sistemas ALD/CTF de las empresas.

Debido a la pandemia, se han incrementado exponencialmente las transacciones en línea, los nuevos usuarios en línea y los nuevos dispositivos, lo que ha dificultado la identificación de riesgos. El uso cada vez mayor de sistemas móviles y en línea por parte de los clientes, y los proveedores de servicios externos puede afectar negativamente la capacidad de telecomunicaciones. Las infraestructuras tecnológicas deben gestionarse de manera eficaz para proporcionar un ancho de banda de telecomunicaciones adicional cuando sea necesario para mantener niveles de servicio adecuados y prevenir los riesgos tecnológicos.

Uno de los delitos con mayor crecimiento durante la pandemia ha sido el robo de identidad, lo que ha resultado traumático para cumplir con la regla número uno de la lucha contra el lavado de dinero: El **conocimiento del cliente (Know Your Customer – KYC)**, porque definitivamente hay algunos procedimientos y procesos de conozca a su cliente que no se pueden utilizar en momentos de pandemia.

La pandemia generó y aceleró los cambios al fomentar el uso de la identidad digital y mejorar las opciones de pago electrónico y digital, aumentando los límites para los pagos sin contacto, las compras en el punto de venta y las billeteras electrónicas y además flexibilizó la verificación de la identidad del cliente al hacerlo de forma remota, eliminando el uso de los métodos tradicionales.

La mayoría de los métodos aprobados para la identificación de los clientes en tiempo de pandemia, incluida la aceptación de documentación escaneada y la confianza en la verificación de terceros, ya están disponibles para las empresas. Las empresas tendrán que evaluar si los controles que tienen son suficientes para mitigar los riesgos específicos que sin duda se harán evidentes a medida que continúe el negocio. Sin embargo, poner en práctica estos controles puede estar plagado de desafíos operativos porque el mensaje de todos los reguladores es que las empresas no deben debilitar sus controles.

Ante esta situación, el Grupo de Acción Financiera Internacional - GAFI desarrolló recientemente una guía sobre Identificación Digital[6] para ayudar a los gobiernos, instituciones financieras, proveedores de servicios de activos virtuales y otras entidades reguladas a determinar si una identificación digital es apropiada para su uso en la debida diligencia del cliente.

**FinCEN Files Leaks**

El 20 de septiembre de 2020, el Consorcio Internacional de Periodistas de Investigación publicó una serie de documentos filtrados de la Financial Crimes Enforcement Network (FinCEN) que es la oficina del Departamento del Tesoro de los Estados Unidos que recopila y analiza información sobre transacciones financieras con el objetivo de combatir el lavado de dinero, la financiación del terrorismo y otros delitos financieros. Los llamados archivos de FinCEN contienen más de 2,100 Reportes de Operaciones Sospechosas (SAR, por sus siglas en inglés) que fueron presentados por instituciones financieras a FinCEN entre 1999 y 2017 (representan menos del 0.02 por ciento de la cantidad total de SAR presentados durante este período) y la cantidad total de transacciones cubiertas por los archivos de FinCEN superó los $2 billones de dólares.

La filtración de los archivos de FinCEN revela una exposición al lavado de dinero en todo el sector financiero. La información revelada en esos archivos indica que el lavado de dinero sigue siendo hoy en día un problema estructural y global importante que debe abordarse. Además, las actividades ilegales reportadas también muestran el creciente nivel de sofisticación detrás de los esquemas de lavado de dinero.

A pesar de los esfuerzos de las instituciones financieras para prevenir las actividades de lavado de dinero, la financiación del terrorismo y otras formas de delitos financieros, la pandemia ha puesto de relieve que aún se necesitan más acciones para mejorar la solidez del marco regulatorio y de cumplimiento de las empresas. El

[6] Ver documento completo en: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

tiempo del cumplimiento técnico ha terminado y las instituciones financieras no pueden darse el lujo de no tener marcos más sistémicos y efectivos.

En particular, las instituciones financieras deberán conectar los puntos entre la información recopilada de la debida diligencia del cliente y los Reportes de Operaciones Sospechosas. Como lado positivo, los informes filtrados muestran que los sistemas de detección y monitoreo están funcionando según lo previsto.

Así mismo, los archivos de FinCEN reafirman la importancia del sector financiero y sus medidas de cumplimiento preventivo en la lucha contra el lavado de dinero y la financiación del terrorismo, ya que es probable que estos temas sigan ocupando un lugar destacado en la agenda pública durante muchos años.

Sin embargo, esta filtración puso de presente las grandes deficiencias del sistema ALD/CFT relacionada con la efectividad de los ROS, el cambio que debe darse en el paradigma de la inteligencia financiera, la seguridad de la información al interior de la Unidades de Inteligencia Financiera (UIF) y el proceso de selección de sus funcionarios como lo analizamos en nuestro artículo.

**Índice AML de 2020 de Basilea**

Con relación al Índice AML de 2020 de Basilea, los hallazgos pusieron de manifiesto los graves problemas de los países relacionados con el Enfoque Basado en Riesgo, la efectividad de las medidas antilavado, las fallas en la identificación de los nuevos riesgos como la trata de personas, los criptoactivos, la financiación del terrorismo, la Financiación de Proliferación de Armas de Destrucción Masiva (FPADM), la falta de visión para tener un enfoque más regional del riesgo LA/FT, las fallas al no hacer más realistas la Evaluación Nacional de Riesgo de cada país, la falta de revisión de la política antilavado de cada país y la falta de colaboración entre las diferentes entidades del estado involucradas en la lucha antilavado, así como los problemas para que el sistema judicial opere efectivamente y genere más condenas por estos delitos o las fallas para la revisión y el control de las Actividades y Profesiones No Financieras Designadas (APNFD).

## Recomendaciones

Por todo lo expuesto anteriormente, queremos plantear algunas recomendaciones para los diferentes actores en la lucha contra el lavado de activos y la financiación del terrorismo:

**Gobiernos**

1. Los gobiernos deberían revisar periódicamente la política antilavado y contra la financiación del terrorismo para adaptarla a los entornos actuales.

2. Los gobiernos deberían mejorar la coordinación Interinstitucional entre las diferentes entidades que luchan contra el lavado de activos y la financiación del terrorismo.

3. El sistema judicial debería mejorar la efectividad, oportunidad y condena de los juicios por los delitos de lavado de activos y financiación del terrorismo, así como los procesos de extinción de dominio.

4. Los gobiernos deberían revisar continuamente la normativa LA/FT de todos los sujetos obligados y controlar efectivamente las Actividades y Profesiones No Financieras Designadas (APNFD).

5. Los gobiernos deben fortalecer los mecanismos de seguridad informática para garantizar que la información sensible de lucha contra estos delitos goce de la reserva, confidencialidad e integridad que se exige a todos los países.

6. Los gobiernos deberían promover las leyes correspondientes para mejorar la normativa ALD/CFT.

**Sujetos obligados**

1. Los sujetos obligados deberían mantener sistemas y controles efectivos, acordes con sus riesgos, para prevenir el lavado de dinero y el financiamiento del terrorismo.

2. Los sujetos obligados deben estar atentos a las nuevas tipologías y deben modificar su entorno de control cuando sea necesario para responder a las nuevas amenazas. Esto debe incluir la notificación oportuna de los Reportes de Operaciones Sospechosas (ROS) de cualquier nueva amenaza.

3. Los sujetos obligados deben incluir revisiones continuas de debida diligencia del cliente o revisiones de alertas de monitoreo de transacciones de clientes de alto riesgo.

4. Los sujetos obligados, cuando necesiten modificar sus controles en respuesta a las circunstancias de la pandemia, deben evaluar claramente los riesgos incluyendo la valoración en cuanto a la probabilidad y el impacto, documentarlos y someterlos a la aprobación de un gobierno corporativo adecuado.

5. Los sujetos obligados deben asegurarse de que sus sistemas funcionen de manera tan eficiente y segura como lo hacían en la era anterior al COVID-19, al mismo tiempo que identifiquen y responden rápidamente a nuevas tácticas criminales potenciales y a los perpetradores de delitos financieros durante la pandemia y cuando la economía se normalice.

6. Los sujetos obligados deberían realizar auditorías de cumplimiento independientes para evaluar los programas ALD/CFT con respecto a estándares internacionales y las recomendaciones del Grupo de Acción Financiera Internacional (GAFI).

7. Los sujetos obligados y las APNFDs deberían revisar sus políticas, manuales, procedimientos para verificar si luego de efectuar un ROS, la relación con la contraparte reportada a la UIF se mantiene, es cancelada y si dicha cancelación se produce oportunamente.

8. Los sujetos obligados deben asegurarse de que la organización haya establecido y comunicado la cultura ética, de control, de cumplimiento y de riesgos en toda la organización.

9. Los sujetos obligados deben asignar los recursos adecuados al sistema ALD/CFT, para acelerar las iniciativas tecnológicas y automatizar los procesos claves del sistema y el monitoreo de operaciones sospechosas de forma segura y remota, como respuesta a una mayor carga de trabajo durante el COVID-19.

10. Los sujetos obligados deben aplicar los avances en tecnología como el blockchain, inteligencia artificial, machine learning para integrarlas a la prevención y control del riesgo de LA/FT.

11. Las empresas pueden comenzar aprovechando la tecnología y los atributos de riesgo empresarial para automatizar los procesos.

**Oficial de Cumplimiento**

1. Los Oficiales de Cumplimiento y en general todas las personas involucradas, deberían mejorar sus competencias y habilidades capacitándose en estándares internacionales como ISO 31000:2018 Gestión de Riesgo, ISO 37001:2016 Gestión Antisoborno, ISO 19600:2014 Gestión de Cumplimiento o certificándose internacionalmente en ALD/CFT.

2. Los Oficiales de Cumplimiento deben revisar sus procesos de análisis, verificación y reporte no solo de los Reportes de Operaciones Sospechosas, tanto consumadas como intentadas, sino de las operaciones inusuales.

3. Los Oficiales de Cumplimiento deben conocer las políticas internas de su empresa y tener un conocimiento y una comprensión exhaustivos de dónde es posible que se produzcan infracciones regulatorias y deben realizar auditorías internas de los procedimientos de su empresa con regularidad. Al monitorear y revisar continuamente las políticas y los procedimientos de la empresa, el Oficial de Cumplimiento debe poder identificar las áreas donde se deben realizar mejoras.

4. Los Oficiales de Cumplimiento deben trabajar en estrecha colaboración con la Alta Gerencia y las unidades comerciales para establecer pautas y poner en práctica los planes de contingencia adecuados sobre cómo responder en caso de que se produzca una infracción de cumplimiento.

5. Los Oficiales de Cumplimiento deben ejercer su trabajo en la compañía con autoridad, autonomía y los recursos adecuados para cumplir con su función y así lograr un programa efectivo de ética y cumplimiento.

**Reguladores**

1. Los reguladores deberían contar con una guía de supervisión que genere seguridad jurídica a los sujetos obligados y capacitarse de forma continua en la normativa internacional ALD/CFT para adecuar la normativa nacional.

2. Los reguladores deberían conocer los diferentes sectores económicos de los sujetos obligados y así emitir la normativa apropiada ALD/CFT.

3. Los reguladores deberían revisar la efectividad del sistema ALD/CFT de los sujetos obligados y no simplemente el cumplimiento formal y documental del sistema.

4. Los reguladores deberían imponer las sanciones correspondientes en caso de incumplimiento por parte de los sujetos obligados y revelar las multas y sanciones impuestas para generar una cultura de cumplimiento.

5. Los reguladores deberían analizar e investigar los nuevos riesgos emergentes como los relacionados con activos virtuales y la trata de personas y su relación con el lavado de activos y la financiación del terrorismo, para emitir una normativa que efectivamente mitigue dichos riesgos.

6. Los reguladores deberían entender lo que significa el Riesgo de Financiación de Proliferación de Armas de Destrucción Masiva (FPADM) en el entorno nacional para luego trabajar de forma mancomunada con los sujetos obligados en la implementación de la normativa en cada uno de los sectores de la economía.

**Unidades de Inteligencia Financiera**

1. Las Unidades de Información Financiera (UIF) deben revisar su trabajo en forma autocrítica y cambiar el paradigma de la investigación financiera.

2. Las UIF deben revisar los procesos internos orientados a garantizar la integridad y seguridad de la información, no solo por la confidencialidad de esta sino para generar en los reportantes la confianza necesaria que les permita cumplir con su obligación legal de reporte en condiciones seguras.

3. Las UIF deben capacitar en forma diferenciada a los sujetos obligados para asegurar la efectividad de los ROS.

4. Las UIF, sin comprometer la confidencialidad de la información, deben compartir la información estadística de los ROS reportados por cada sector de los sujetos obligados.

5. Las UIF deben verificar la efectividad y calidad de los ROS, para hacer las mejoras necesarias en el sistema.

6. Los reguladores y las UIF deberían establecer nuevos programas de capacitación cruzada y dar a conocer nuevas tipologías de acuerdo con la realidad digital y tecnológica en la que nos movemos.

Finalmente, los gobiernos, los reguladores, las UIF y los sujetos obligados debemos sincerarnos y tomarnos la foto de la realidad actual del sistema ALD/CFT, sin filtros, sin Photoshop, sin mentiras y que la sinceridad de esa foto nos permita tomar las medidas necesarias para mejorar ese modelo antilavado y contra la financiación del terrorismo y luchar efectivamente contra esos delitos.

***Juan Pablo Rodríguez C.**
Abogado Penalista
Escritor, conferencista y consultor internacional.
Certificado en Compliance CESCOM® de la Asociación Española de Compliance, ASCOM, 2020
Certified Lead Auditor, Lead Implementer y Trainer en ISO 37001 Gestión Antisoborno, PECB, 2020
Certified Professional in Anti-Money Laundering - CPAML de FIBA (Florida International Bankers Association).

Certified on Governance, Risk Management and Compliance Professional (GRCP) y GRC Fundamentals de Open Compliance and Ethics Group (OCEG), 2016
Presidente y Socio de RICS Management.
www.ricsmanagement.com
jrodriguez@ricsmanagement.com

****René M. Castro V.**
Contador Público con Magister en Contabilidad y Auditoría de Gestión de la Universidad de Santiago de Chile.
Escritor, conferencista y consultor internacional.
Certified Trainer y Lead Compliance Manager en ISO 19600 Gestión de Cumplimiento, PECB, 2020
Certified on Financial Services and Market Regulation, London School of Economics, (LSE), 2016
Certified on Corporate Compliance and Ethics, New York University, 2015.
Vicepresidente & Socio RICS Management
www.ricsmanagement.com
rcastro@ricsmanagement.com

*****Camilo A. Rueda B.**
Profesional en Finanzas y Relaciones Internacionales de la Universidad Externado de Colombia con estudios de Maestría en Seguridad y Defensa Nacional de la Escuela Superior de Guerra.
Anti-Money Laundering Certified Associate (AMLCA) por Florida International Bankers Association - FIBA
Certificado en Compliance CESCOM® de la Asociación Española de Compliance, ASCOM, 2020.
Escritor, conferencista y consultor internacional.
Consultor asociado de RICS Management
www.ricsmanagement.com
crueda@ricsmanagement.com