

Bank of America: cuando el sistema AML deja de ver el riesgo**La sanción de octubre de 2026 y sus lecciones para los oficiales de cumplimiento**

*Juan Pablo Rodríguez C.

**René M. Castro V.

***Camilo A. Rueda B.

La acción coordinada contra Bank of America (BoA) merece atención más allá de la magnitud de la sanción. La resolución describe deficiencias que persistieron durante años, pese a advertencias internas, pruebas de control y un requerimiento de autoridad previo. Su principal valor para la función de cumplimiento consiste en mostrar cómo decisiones aparentemente técnicas -umbrales, reglas de supresión, cobertura de productos y métricas operativas- pueden convertirse en fallas de gobierno y en reportes tardíos de actividad sospechosa.

1. El caso

El 13 de octubre de 2026, Unidad de Inteligencia Financiera de Estados Unidos (Financial Crimes Enforcement Network, FinCEN) anunció una sanción civil de US\$1.200 millones contra BoA, por incumplimientos de la Ley de Secreto Bancario (Bank Secrecy Act, BSA) y deficiencias en la identificación, investigación y comunicación de operaciones sospechosas. La sanción contempla un crédito de US\$750 millones correspondiente a la multa impuesta, por los mismos hechos en materia de prevención del lavado de dinero, por la Oficina del Contralor de la Moneda (OCC).

En consecuencia, ambos componentes no deben sumarse íntegramente como sanciones independientes: el banco debe pagar US\$450 millones a FinCEN y US\$750 millones a la OCC. Por separado, la Oficina de Control de Activos Extranjeros (Office of Foreign Assets Control, OFAC) acordó con la entidad un pago de US\$11,7 millones por 475 aparentes infracciones de los programas estadounidenses de sanciones económicas. En conjunto, las medidas anunciadas superan los US\$1.210 millones y reflejan la intervención coordinada de las autoridades frente a deficiencias tanto en los controles contra el lavado de dinero como en el cumplimiento de las sanciones financieras.

En cuanto a la gravedad de las deficiencias, las autoridades determinaron que el banco no reportó oportunamente a FinCEN operaciones sospechosas por más de US\$5.000 millones, de las cuales más de US\$1.000 millones estaban relacionadas con riesgos prioritarios para la seguridad nacional y otras formas de financiación ilícita. Entre estos riesgos se encontraban indicios de redes chinas de lavado de dinero, fraude y posibles operaciones de lavado mediante el comercio, con vínculos relevantes con la frontera suroccidental de Estados Unidos. La investigación también identificó deficiencias en el sistema de monitoreo transaccional, la debida diligencia de clientes y de cuentas de corresponsalía bancaria de entidades financieras extranjeras, así como retrasos acumulados en la investigación y presentación de reportes de actividades sospechosas.

Según la OCC, el sistema de monitoreo no permitió supervisar adecuadamente transacciones por billones de dólares, mientras que la falta de escalamiento de alertas, las insuficiencias en la capacitación del personal y las debilidades de la auditoría interna impidieron detectar o corregir oportunamente problemas conocidos por la entidad. Es importante precisar que los más de US\$5.000 millones corresponden al valor de las operaciones sospechosas cuyo reporte fue tardío, no a una determinación de que la totalidad de esos fondos procediera de actividades delictivas.

Un elemento adicional es la persistencia de las deficiencias pese a las medidas correctivas previamente exigidas. En diciembre de 2024, la OCC ya había emitido una orden para que BoA subsanara las debilidades de su programa de cumplimiento de la BSA y de prevención del lavado de dinero (anti-money laundering, AML). Sin embargo, las autoridades concluyeron que la entidad no había implementado satisfactoriamente varias medidas relevantes y que continuaban existiendo fallas en la identificación y el escalamiento de operaciones sospechosas. Asimismo, el acuerdo con OFAC puso de manifiesto debilidades distintas, aunque relacionadas con el entorno general de control: procesamiento de pagos vinculados con bancos bloqueados, priorización inadecuada de alertas, actualización tardía de listas de sanciones y errores en la gestión de cuentas asociadas con personas bloqueadas.

Por tanto, el caso trasciende el importe de las sanciones y evidencia las consecuencias de no corregir de manera efectiva deficiencias conocidas. Su principal enseñanza para los oficiales de cumplimiento es que la existencia formal de políticas, procedimientos y controles como ingredientes de un sistema, no basta para demostrar la eficacia del programa: se requiere evidencia verificable de que los controles identifican los riesgos relevantes, generan investigaciones oportunas y conducen a decisiones correctivas proporcionales a los hallazgos.

2. ¿Qué se sancionó y cómo deben leerse las cifras?

Para comprender el alcance económico, es necesario distinguir las medidas coordinadas. FinCEN fijó la sanción civil nominal en US\$1.200 millones por violaciones de la BSA (incumplimiento administrativo); el pago de US\$750 millones al OCC se acredita contra ese importe, de modo que US\$450 millones se pagan a FinCEN. A ello se suma el acuerdo separado con OFAC por US\$11.662.930. En conjunto, y sin duplicar el crédito entre autoridades, las medidas anunciadas superan US\$1,21 mil millones. El OCC describió su sanción como la mayor de su historia, mientras que el Tesoro calificó la medida conjunta como la tercera mayor sanción de su historia.

Los hechos descritos en la orden de FinCEN cubren, en términos generales, el periodo comprendido entre el 1 de enero de 2018 y el 1 de julio de 2025. BoA admitió haber violado deliberadamente la BSA en el sentido civil aplicable a esa norma, que puede comprender conductas de indiferencia temeraria o ceguera deliberada. Esta admisión no equivale a una condena penal ni permite afirmar que cada operación cuestionada procediera de un delito. Los más de US\$5.000 millones corresponden a actividad sospechosa no reportada oportunamente; aproximadamente US\$1.000 millones estaban vinculados con riesgos prioritarios de financiación ilícita y seguridad nacional.

3. El fallo central: un sistema de monitoreo que filtraba el riesgo

La orden de FinCEN ubica en el centro del problema el sistema propietario Event Processor (EP), implementado desde 2010 para agrupar alertas, asignar puntajes y enviar a investigación los grupos que alcanzaran un umbral de 20 puntos. Ese umbral se había fijado inicialmente por criterio de los responsables, sin respaldo empírico suficiente. Como el sistema consolidaba señales durante periodos prolongados, ciertas actividades podían llegar a investigarse más de un año después de las transacciones; además, una parte material de los reportes se presentó más de seis meses después de la actividad relevante.

El problema no consistía únicamente en la antigüedad de la herramienta. Los pesos de algunos factores de riesgo no reflejaban adecuadamente su capacidad para identificar operaciones que debían investigarse;

además, se modificaban o suprimían alertas sin controles de gobierno y pruebas suficientes. Las deficiencias detectadas en ejercicios de prueba tampoco se corrigieron de forma efectiva. En varios años, más de un tercio de las investigaciones de actividad sospechosa tuvo origen en requerimientos policiales, referencias de otras entidades o procesos manuales, en lugar de controles automatizados propios. En la práctica, fuentes externas identificaban señales que el banco debía detectar de manera proactiva.

Este caso ilustra el riesgo de confundir eficiencia operativa con efectividad preventiva. Un sistema que genera menos alertas o una carga de trabajo más manejable no es necesariamente mejor si excluye señales relevantes. Tras modificar parámetros en diciembre de 2023, una revisión retrospectiva de alcance limitado identificó casi US\$4.000 millones en actividad sospechosa que, con los umbrales anteriores, no habría sido investigada ni reportada a tiempo. Una revisión de terceros realizada en 2025 seguía encontrando deficiencias. Por tanto, la recalibración no puede considerarse exitosa únicamente porque reduzca alertas o tiempos de procesamiento: debe demostrarse que mejora la detección del riesgo.

4. Debida diligencia y señales de riesgo que no cambiaron decisiones

Las fallas también afectaron la debida diligencia del cliente (CDD). Dos clientes corporativos del sector de subastas de vehículos en línea recibían grandes volúmenes de instrumentos negociables -incluidos giros monetarios adquiridos en otras instituciones- y pagos efectuados por terceros cuyo vínculo con el comprador registrado no siempre era transparente. La orden identifica más de US\$600 millones en operaciones sospechosas relacionadas con vehículos recuperados, parte de ellas con conexión con la frontera suroccidental de Estados Unidos. El banco no monitoreaba adecuadamente ciertos depósitos de instrumentos negociables, pese a conocer señales de riesgo en clientes de esa actividad.

La cuestión no es que la compraventa internacional de vehículos sea sospechosa por sí misma, sino que la combinación de pagos de terceros, instrumentos monetarios secuenciales, montos redondos, compradores internacionales y cambios de comportamiento exigía una revisión sustantiva del perfil de riesgo. La orden también describe patrones compatibles con tipologías atribuidas a redes chinas de lavado de dinero, fraude y posible lavado basado en el comercio. En estos escenarios, la debida diligencia debe permitir comprender quién aporta realmente los fondos, por qué se utilizan determinados instrumentos, cuál es el propósito económico de la operación y quién obtiene el beneficio final.

La resolución del OCC identificó, además, deficiencias de capacitación y competencias en el oficial BSA y su equipo, así como debilidades en la función de auditoría independiente. La responsabilidad, por tanto, no se limita al modelo de monitoreo: involucra a la dirección que asigna recursos, las áreas comerciales que mantienen las relaciones, los responsables que aceptan riesgos, la función de cumplimiento que debe contar con autoridad efectiva y la auditoría que debe verificar los resultados con independencia.

5. Una segunda señal: sanciones y antecedente regulatorio de 2024

El acuerdo de OFAC es jurídicamente distinto de la sanción principal de BSA/AML. Comprende 475 aparentes infracciones relacionadas con programas de sanciones relativos a Rusia, Bielorrusia, Irán, Birmania, Somalia, narcóticos y terrorismo global. Entre los problemas señalados figuran pagos que involucraron bancos bloqueados, priorización insuficiente de alertas de coincidencia con personas designadas, actualización tardía de listas y errores humanos en el tratamiento de cuentas. OFAC consideró que las infracciones no eran graves,

pero observó que en gran medida no fueron autodenunciadas voluntariamente. El caso aconseja integrar la gestión de riesgos AML y de sanciones, sin confundir sus marcos jurídicos y obligaciones específicas.

El antecedente del OCC añade una dimensión de persistencia. En diciembre de 2024, el regulador dictó una orden de cese y desistimiento por reportes tardíos de operaciones sospechosas, fallas de debida diligencia y deficiencias en controles internos, gobierno, pruebas independientes y capacitación. La orden exigía acciones correctivas y revisiones históricas para determinar si correspondía presentar reportes adicionales. En octubre de 2026, las autoridades concluyeron que persistían brechas importantes. La secuencia demuestra que aprobar un plan de remediación, contratar consultores o anunciar inversiones no acredita por sí mismo la corrección de las causas raíz: es necesario probar que los controles funcionan de manera sostenida.

6. Comparación con otros casos relevantes

Los siguientes casos permiten identificar patrones comparables en la gestión del riesgo de lavado de dinero. Las cifras no son estrictamente homogéneas: algunas corresponden a sanciones administrativas y otras incluyen acuerdos penales, decomisos o medidas de varias autoridades. En consecuencia, el cuadro no pretende establecer un ranking de gravedad, sino mostrar similitudes en las fallas de monitoreo, reporte, debida diligencia y supervisión.

Caso	Medida económica	Paralelo principal
TD Bank (2024)	≈ US\$3.000 millones en medidas coordinadas; FinCEN: US\$1.300 millones.	Deficiencias prolongadas, grandes volúmenes sin monitoreo suficiente, acumulación de alertas y priorización de crecimiento sobre controles. Se impuso un monitor independiente por cuatro años.
U.S. Bank / U.S. Bancorp (2018)	US\$528 millones en acuerdo penal diferido; medida adicional de FinCEN.	La institución limitaba alertas de acuerdo con la capacidad de investigación, no con el riesgo. Pruebas bajo los umbrales identificaron operaciones que debieron escalar.
Capital One (2021)	US\$390 millones de FinCEN.	Fallas asociadas a clientes de alto riesgo del negocio de cambio de cheques y omisiones de reportes. Ilustra cómo el riesgo puede concentrarse en una línea de negocio.
HSBC (2012)	US\$1.256 millones de decomiso, dentro de un acuerdo penal diferido.	Deficiencias AML, debida diligencia de corresponsales y operaciones relacionadas con países sancionados; se impusieron medidas de supervisión reforzada.
Merrill Lynch (2026)	US\$7,5 millones de sanción de la SEC.	La entidad dependía del programa AML corporativo de Bank of America, pero no investigó ciertos grupos de alertas por debajo del umbral ni presentó reportes requeridos.

La comparación refuerza una conclusión común: las sanciones de mayor relevancia no suelen derivarse de un error aislado, sino de brechas que se mantienen en el tiempo, controles que dejan fuera segmentos del negocio y señales que no se convierten en decisiones oportunas. La existencia de tecnología, políticas o una función de cumplimiento centralizada no sustituye la responsabilidad de cada entidad de demostrar que detecta y reporta las operaciones que le corresponde identificar.

7. Lecciones prácticas para los oficiales de cumplimiento

Las lecciones del caso son aplicables más allá de la banca. Cambia la naturaleza de los productos y los canales, pero permanece la necesidad de conocer a los clientes, entender el propósito económico de las operaciones, identificar desviaciones y documentar las decisiones. Para convertir estas lecciones en mejoras verificables, conviene concentrarse en los siguientes ámbitos de gestión.

- a. **Diseño del monitoreo basado en riesgo.** La entidad debe mantener un inventario actualizado de productos, canales, tipos de operación y poblaciones cubiertas, y comprobar que todos estén integrados en el monitoreo según su riesgo. Giros, tarjetas, pagos de terceros, instrumentos negociables y transferencias internacionales no deben quedar excluidos por limitaciones heredadas de sistemas o por una implantación tecnológica incompleta.
- b. **Validación de los umbrales y las exclusiones.** Las pruebas deben revisar no solo las alertas que el sistema genera, sino también las operaciones descartadas, suprimidas o situadas por debajo de los umbrales. El análisis de falsos negativos, los resultados de muestras retrospectivas y la justificación empírica de las ponderaciones permiten evaluar si los cambios mejoran la detección. Cada recalibración debe tener responsable, aprobación, trazabilidad y evaluación posterior.
- c. **Medición de la oportunidad y la cobertura.** Los indicadores deben abarcar la antigüedad de alertas y expedientes, los tiempos de análisis y reporte, los casos pendientes, la cobertura por producto y los resultados de las pruebas independientes. Reducir la carga de trabajo no es una meta suficiente si aumenta el riesgo no detectado. Cuando los recursos resulten insuficientes, la brecha debe escalarse a la dirección, en lugar de reducir silenciosamente el alcance del control.
- d. **Debida diligencia continua.** El perfil del cliente debe contrastarse con el comportamiento observado y actualizarse cuando cambien los volúmenes, los países, los pagadores, los instrumentos o el modelo de negocio. Es necesario comprender quién aporta realmente los fondos, el origen y destino de estos, el beneficiario final y la lógica económica de la actividad. Las señales relevantes deben activar una revisión sustantiva y, cuando corresponda, restricciones, escalamiento o terminación de la relación.
- e. **Independencia y escalamiento.** Cumplimiento debe poder elevar alertas y recomendaciones sin que las áreas comerciales puedan neutralizarlas indefinidamente. El gobierno interno debe definir rutas de escalamiento a la alta dirección y al órgano de administración, con registro de las decisiones, responsables, plazos y aceptación expresa de los riesgos residuales. La independencia formal es insuficiente si la función carece de autoridad, recursos o acceso a los órganos de decisión.
- f. **Aseguramiento independiente y calidad de datos.** La auditoría debe evaluar la efectividad de los controles mediante pruebas basadas en riesgo y evidencia verificable, no limitarse a comprobar la existencia de manuales. La integridad, calidad, trazabilidad y oportunidad de los datos son parte del control AML. Asimismo, las pruebas deben revisar que los resultados de monitoreo lleguen a quienes investigan y deciden, sin pérdida de información relevante durante la transferencia entre sistemas.
- g. **Remediación demostrable.** Cada hallazgo debe vincularse con una causa raíz, una acción concreta, un responsable, una fecha de cumplimiento, un indicador de efectividad y una prueba posterior independiente. Cerrar una tarea no equivale a cerrar un riesgo. En cooperativas, remesadoras, juegos de azar, construcción y servicios profesionales, la forma de los controles variará, pero el criterio permanece: comprender los flujos, las contrapartes, las señales atípicas y la respuesta adoptada.

8. Conclusión

El caso BoA demuestra que un programa AML puede fracasar cuando sus controles no representan los riesgos reales, cuando las pruebas identifican fallas que no se corrigen y cuando los objetivos operativos terminan

desplazando la detección y el reporte oportuno de actividad sospechosa. La escala de la entidad y su inversión tecnológica no sustituyen una cultura de cumplimiento ni una supervisión efectiva. La pregunta decisiva para el oficial de cumplimiento no es si existen políticas, sistemas y capacitaciones, sino si la organización puede demostrar, mediante datos confiables, pruebas independientes y decisiones oportunas, que identifica, investiga y escala los riesgos que afirma gestionar.

9. Fuentes principales

El análisis se apoya prioritariamente en órdenes y comunicados oficiales de las autoridades estadounidenses, complementados con decisiones de cumplimiento de otros bancos que permiten identificar patrones comparables.

- [1] [FinCEN. Consent Order In the Matter of Bank of America, N.A. \(13 de octubre de 2026\). Documento íntegro, 95 páginas.](#)
- [2] [Departamento del Tesoro de Estados Unidos. U.S. Treasury Announces Record Enforcement Actions Against Bank of America \(13 de octubre de 2026\).](#)
- [3] [OCC. OCC Imposes \\$750 Million Assessment Against Bank of America for Deficient BSA/AML Compliance \(13 de octubre de 2026\).](#)
- [4] [OFAC. Settlement Agreement between OFAC and Bank of America, N.A. \(13 de octubre de 2026\).](#)
- [5] [OCC. OCC Issues Cease and Desist Order Against Bank of America for BSA Deficiencies \(23 de diciembre de 2024\).](#)
- [6] [FinCEN. FinCEN Assesses Record \\$1.3 Billion Penalty against TD Bank \(10 de octubre de 2024\).](#)
- [7] [Departamento de Justicia de Estados Unidos. United States of America v. TD Bank US Holding Company.](#)
- [8] [Departamento de Justicia de Estados Unidos. Criminal Charges Against U.S. Bancorp for Violations of the Bank Secrecy Act \(15 de febrero de 2018\).](#)
- [9] [FinCEN. \\$390,000,000 Enforcement Action Against Capital One, National Association \(15 de enero de 2021\).](#)
- [10] [Departamento de Justicia de Estados Unidos. HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations \(11 de diciembre de 2012\).](#)
- [11] [SEC. SEC Institutes Settled Order Against Merrill Lynch for Failing to File Suspicious Activity Reports \(29 de junio de 2026\).](#)

*Juan Pablo Rodríguez C.

Abogado Penalista

Escritor, conferencista y consultor internacional.

Par Académico de CONEAUPA.

Certificado en Blockchain y Disrupción Tecnológica del MIT.

Certificado en Compliance CESCO® 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 of Open Compliance and Ethics Group (OCEG), 2016.

Course Completion *Certified Artificial Intelligence Manager (CAIM)* de PECB (Canadá)

Autor del libro *Compliance, lavado de activos y corrupción: guía de prevención y control*. Editorial Tirant lo Blanch.

Presidente y Socio de RICS Management.

jrodriguez@ricsmanagement.com

****René M. Castro V.**

Contador Público con Magister en Contabilidad y Auditoría de Gestión de la Universidad de Santiago de Chile.

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.

Course Completion *Certified Artificial Intelligence Manager (CAIM)* de PECB (Canadá)

Escritor, conferencista y consultor internacional.

Vicepresidente & Socio RICS Management.

rcastro@ricsmanagement.com

*****Camilo A. Rueda B.**

Profesional en Finanzas y Relaciones Internacionales con estudios de Maestría en Seguridad y Defensa Nacional.

Anti-Money Laundering Certified Associate (AMLCA) por Florida International Bankers Association - FIBA

Certificado en Compliance CESCO® de la Asociación Española de Compliance, ASCOM, 2020.

Course Completion *Certified Artificial Intelligence Manager (CAIM)* de PECB (Canadá)

Escritor, conferencista y consultor internacional.

Socio & Director RICS Management Guatemala.

crueda@ricsmanagement.com