COMPLIANCE 360
ExecutiveEducation

ENTREVISTAS C360:

Manú Hersch Garcia

FinCrime Compliance
Team Leader
Lemon

junio, 2026

¿Quién es Manú?

Profesional en compliance, prevención de delitos financieros y regulación internacional, con experiencia en sectores fintech, e-commerce y estudios jurídicos de primer nivel. Actualmente se desempeña como Compliance Team Leader en Lemon, donde es responsable global del Programa AML/CTF. Previamente, formó parte del equipo de Mercado Libre como Analista Senior de Riesgo y Cumplimiento, liderando proyectos en materia de AML, sanciones, anticorrupción, ética corporativa, regulaciones transfronterizas y soluciones de pagos y criptoactivos. Con una trayectoria que inició en el ámbito legal, trabajó en firmas como Bruchou & Funes de Rioja y Governance Latam, especializándose en programas de compliance penal, investigaciones internas y delitos económicos. Su experiencia combina la práctica jurídica con la consultoría y la gestión estratégica del riesgo,aportando una mirada integral para fortalecer la ética, la integridad y la transparencia en las organizaciones.

DISCLAIMER

Las opiniones expresadas en esta entrevista son exclusivamente personales y no reflejan necesariamente la postura, visión o políticas de las organizaciones en las que he trabajado anteriormente ni de la empresa con la que colaboro actualmente.

Cualquier afirmación debe entenderse en el contexto de una perspectiva individual y no como una declaración institucional.

Entrevista | Manú Hersch Garcia

1. Desde tu experiencia en fintech, e-commerce y ahora en el ecosistema cripto, ¿Cuáles son las principales diferencias prácticas entre gestionar compliance en modelos tradicionales y hacerlo en plataformas Web3, donde la velocidad, la descentralización y la trazabilidad plantean nuevos desafíos?

La diferencia más inmediata que noté al pasar de modelos tradicionales al ecosistema Web3 es que en los primeros, compliance opera sobre estructuras relativamente predecibles: hay intermediarios conocidos, flujos de datos centralizados y marcos regulatorios consolidados. En cripto, esa previsibilidad desaparece. Las operaciones ocurren en tiempo real, sin fronteras, y muchas veces sin un responsable institucional claro del otro lado.

Lo que más me impactó al hacer esa transición no fue la complejidad técnica de la blockchain en sí, sino la velocidad a la que el entorno cambia. Una tipología de fraude que hoy no existe puede estar activa mañana, porque los actores maliciosos también iteran rápido. Eso obliga a que el área de compliance deje de ser reactiva y empiece a pensar como una unidad de inteligencia.

La trazabilidad en blockchain es, paradójicamente, tanto una ventaja como un desafío. Podés seguir cada transacción en la blockchain, pero sin las herramientas y el criterio analítico adecuados, esa cantidad de información se vuelve ruido. La clave está en saber qué mirar y por qué, no en tener acceso a todo.

Lo que aprendí en estos años es que compliance en Web3 no es una versión más difícil del compliance tradicional: es un paradigma distinto. Requiere combinar la rigurosidad jurídica del mundo regulado con la agilidad y la mentalidad de producto del mundo tech. Esa combinación no es fácil de encontrar, pero es la que realmente hace la diferencia.

2. En el contexto de AML/CTF aplicado a criptoactivos, ¿Qué errores estructurales observas con mayor frecuencia en los programas de cumplimiento, y qué elementos consideras críticos para que un esquema de cripto-AML sea realmente efectivo y no meramente defensivo?

El error más frecuente que veo es tratar AML/CTF como un ejercicio de documentación. Se construyen políticas robustas, se implementan herramientas de screening, se generan reportes, pero todo queda en la superficie. El programa existe para cumplir una auditoría, no para detectar ni prevenir. Esa lógica defensiva es, en mi experiencia, el mayor riesgo estructural que puede tener una organización.

Un segundo problema es la desconexión entre las herramientas y las personas que las operan. En cripto, muchas organizaciones invierten en plataformas de blockchain analytics sin desarrollar el criterio interno para interpretarlas. Una alerta sin contexto no sirve de nada. Lo que diferencia un programa efectivo es la capacidad de construir narrativa alrededor de los datos: entender qué está pasando realmente, no solo marcar una casilla.

Lo que considero crítico para que un esquema de cripto-AML sea genuinamente efectivo es que esté anclado en una matriz de riesgo actualizada y viva, no en una foto estática de hace dos años. El perfil de riesgo en Web3 muta constantemente, y el programa tiene que mutar con él. Eso implica revisar tipologías, actualizar señales de alerta y, sobre todo, mantener un diálogo permanente entre el área de compliance y los equipos de producto y tecnología.

3. Desde tu rol liderando auditorías e investigaciones en entornos Web3, ¿cómo debería evolucionar la auditoría interna en empresas cripto para convertirse en una herramienta que anticipe riesgos, detecte patrones y fortalezca la toma de decisiones, más allá del cumplimiento formal?

La auditoría interna en empresas cripto todavía está, en muchos casos, atrapada en una lógica de verificación: ¿se cumplió el proceso? ¿existe la política? Ese enfoque tiene valor, pero es insuficiente en un ecosistema donde los riesgos emergen más rápido de lo que cualquier manual puede anticipar.

Lo que vi en mi experiencia es que las auditorías más útiles no son las que encuentran lo que faltó, sino las que logran leer patrones antes de que se conviertan en problemas. Eso requiere incorporar análisis de datos on-chain como parte del proceso auditor, no como un complemento opcional. La información está en la blockchain; la pregunta es si el equipo tiene la capacidad de interrogarla bien.

Pero más allá de las herramientas, el cambio más importante es de posicionamiento. La auditoría interna tiene que dejar de ser percibida como una instancia de control y empezar a funcionar como un socio estratégico de la dirección. Eso implica que sus hallazgos alimenten decisiones de negocio, no solo planes de remediación. En un sector tan dinámico como cripto, esa conexión entre auditoría y estrategia puede ser una ventaja competitiva real.

Escanea el código QR o haz clic en él para acceder a una MasterClass asincronica con Manú

4. En tu experiencia investigando fraudes y operaciones sospechosas en cripto y pagos digitales, ¿qué competencias —más allá de lo técnico— consideras indispensables para que un equipo de compliance pueda interpretar señales de riesgo complejas y no caer en falsos positivos o enfoques puramente automatizados?

La automatización es necesaria, pero no suficiente. Un sistema de alertas bien calibrado puede procesar miles de transacciones por minuto, pero no puede entender el contexto detrás de un comportamiento. Esa es exactamente la brecha que un equipo humano tiene que cubrir, y para eso se necesitan competencias que no aparecen en ningún manual técnico.

La primera es el pensamiento crítico aplicado a datos. No alcanza con saber leer un reporte; hay que poder cuestionarlo. ¿Por qué se disparó esta alerta? ¿Qué más está pasando alrededor de esta operación? ¿Esto es realmente sospechoso o es un patrón legítimo que el sistema no reconoce? Ese tipo de razonamiento es lo que separa un equipo que gestiona alertas de uno que realmente investiga.

La segunda es la capacidad de construir narrativa. En una investigación, los datos sueltos no dicen nada. Lo que importa es la historia que conecta esos datos: quién, cuándo, con qué frecuencia, hacia dónde. Esa habilidad narrativa es clave tanto para tomar decisiones internas como para comunicarlas a reguladores o a la dirección.

Y la tercera es curiosidad genuina y olfato. Los mejores investigadores que conocí no esperaban que el sistema les dijera qué buscar; iban ellos a buscarlo. Esa actitud proactiva es difícil de entrenar, pero es la que más impacto tiene en la calidad de un equipo.

5. Mirando la evolución del sector cripto en América Latina, ¿qué decisiones estratégicas deberían empezar a tomar hoy las organizaciones —y los líderes de compliance— para construir sistemas de gestión robustos, creíbles y alineados con estándares globales, incluso antes de que la regulación sea plenamente clara?

La tentación en contextos de regulación incipiente es esperar. Esperar que el regulador defina, que el mercado madure, que aparezca un estándar claro. En mi experiencia, esa es exactamente la decisión que más cara le sale a una organización cuando la regulación finalmente llega.

Lo que recomendaría es anclar el programa en estándares internacionales desde el primer día, independientemente de lo que exija la normativa local. Las recomendaciones del GAFI, los marcos de la IOSCO, las mejores prácticas de jurisdicciones más maduras: todo eso está disponible y ofrece una hoja de ruta sólida. Las organizaciones que lo hacen no solo están mejor preparadas regulatoriamente; también generan más confianza en inversores, socios y usuarios.

La segunda decisión estratégica es invertir en talento especializado antes de necesitarlo urgentemente. En América Latina hay escasez real de perfiles que combinen conocimiento regulatorio con comprensión del ecosistema cripto. Construir ese equipo lleva tiempo, y hacerlo bajo presión regulatoria es mucho más costoso y riesgoso.

Y la tercera, que muchas veces se subestima, es cultivar una relación proactiva con los reguladores. No esperar a ser convocado, sino participar, aportar perspectiva técnica, estar presente en los espacios donde se diseña la regulación. En un sector tan nuevo, quienes se sientan a la mesa tienen la posibilidad real de influir en cómo se construyen las reglas.