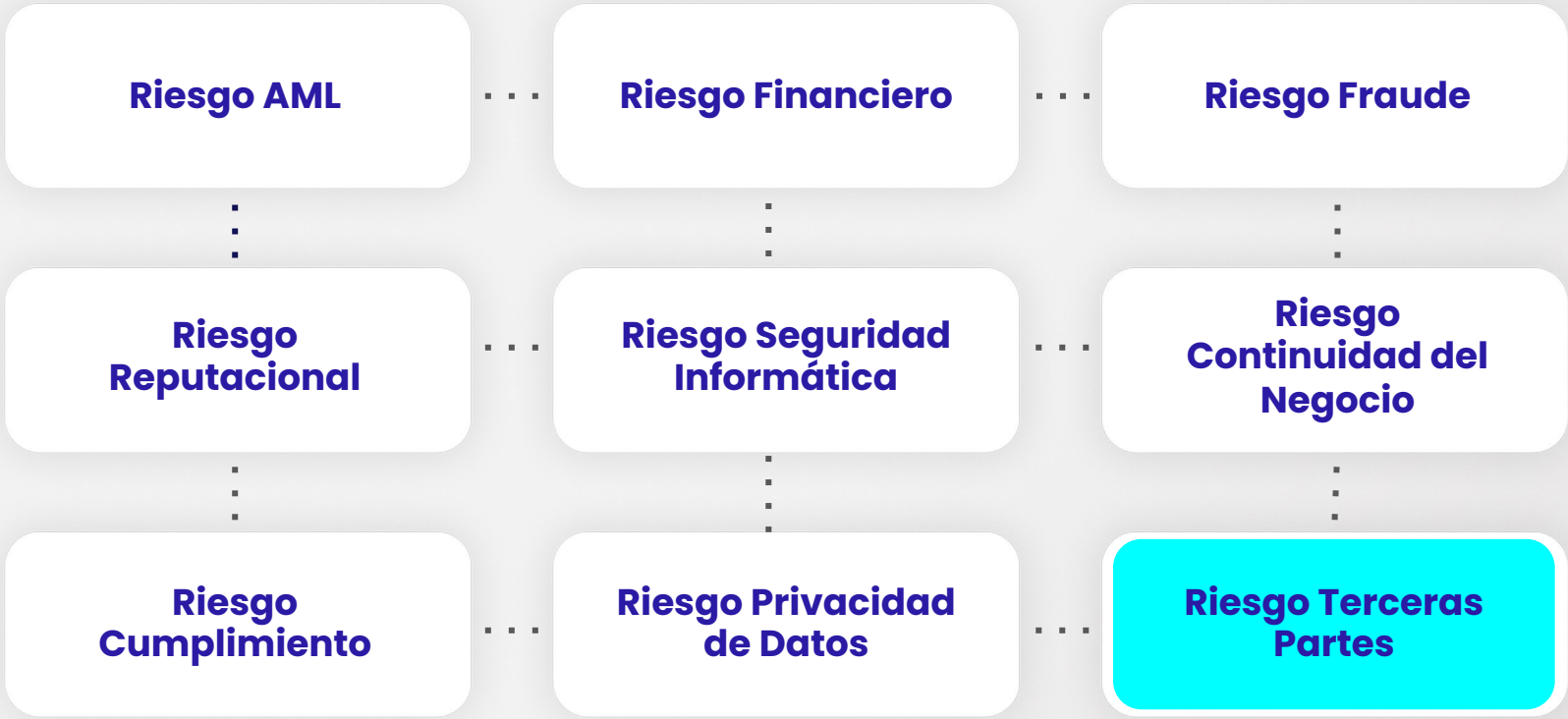
XXVII CONGRESO HEMISFÉRICO PANAMÁ 2023

16-17-18 DE AGOSTO

BIENVENIDOS AL

CONGRESO HEMISFÉRICO PARA LA PREVENCIÓN DE BLANQUEO DE CAPITALES, FINANCIAMIENTO DEL TERRORISMO Y DE LA PROLIFERACIÓN DE ARMAS DE DESTRUCCIÓN MASIVA

Riesgo Holístico



Entidades Cripto y más

Exchanges Centralizadas vs. Descentralizadas

	CEX	DEX
Centralización	Opera a través de una entidad centralizada, que hace de intermediaria.	Opera a través de smart contracts, sin intermediarios.
Moneda	Se permiten transacciones con dinero fiduciario. Se ofrecen menos activos virtuales.	No se permiten transacciones con dinero fiduciario. Se ofrecen más activos virtuales.
Control sobre los activos	La exchange centralizada controla el acceso a los activos virtuales (el Usuario no tiene su clave privada).	El Usuario tiene control sobre sus activos virtuales (tiene su clave privada).
Privacidad/ anonimato	La entidad centralizada puede estar sujeta a cumplir con normativa PLA/FT y llevar a cabo un KYC y debida diligencia de clientes.	En general, no hay un ente centralizado que esté sujeto a normativa de PLA/FT. No se requiere un KYC a los Usuarios.

Riesgos de las Entidades Descentralizadas

→ No exigen que los Usuarios pasen por un KYC

→ No monitorean la actividad de sus Usuarios desde una perspectiva de PLA/FT.

→ Ofrecen una gran cantidad de activos virtuales y no realizan "coin risk assessments" → posibilidad de que ofrezcan monedas privadas (ej. Monero).

→ No tienen la custodia de los activos virtuales de los Usuarios. En un caso de terrorismo/sanciones, no podrían congelar los fondos.

Peer-to-Peer (P2P) Exchange

Las exchanges peer-to-peer permiten comprar criptomonedas a vendedores privados.

En general, los requisitos de KYC y AML son más laxos.

Posibilidad de que se acuerden términos por fuera de la plataforma (sobre los cuales la exchange no tiene visibilidad) → complejiza el monitoreo.

OTC Cripto

Operaciones Over the Counter son aquellas que se realizan a medida de las partes.

En una operación OTC se negocian las condiciones bilateralmente mientras que un pequeño inversor tiene que conformarse con la situación tal como está.

Menos cantidad de operaciones de mayor volumen.

Grandes operaciones ofrecen una conveniente cobertura para la introducción de fondos ilícitos.

“Crypto As a Service”

Productos Cripto

Productos

- Compraventa de activos virtuales
- Préstamos
- Tarjeta prepaga nominada
- Tarjeta de crédito
- Trading
- Peer-to-peer (P2P)
- Crypto as a Service (B2B)
- DeFi
- Donaciones
- Gift cards
- Non-fungible tokens
- Over The Counter (OTC)
- Tarjeta prepaga innominada
- Servicios de remesa internacional (moneda fiduciaria)
- Swaps

¿Qué tienen en común todas estas entidades?

Todas **necesitan** un Programa de Cumplimiento

Gestión de Riesgos en el mundo cripto

Componentes Clave de un Programa de PLA/FT (VASPs)

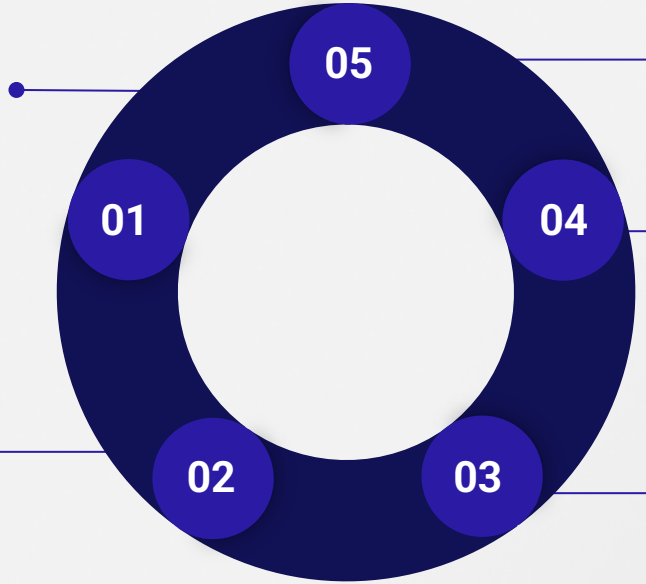
1. Evaluación de Riesgos

Comprende tanto la auto-evaluación de riesgos como la evaluación de clientes/partners.

2. Debida Diligencia del Cliente

Incluye:

a) Conocimiento del cliente (KYC)
b) Screening contra listas PEP y de Sanciones
c) Monitoreo transaccional (KYT)



5. Capacitación

4. Travel Rule

3. Reporte de Actividad/ Operación Sospechosa

Evaluación de Riesgos: Metodología

Riesgo Inherentes

1. Factor Clientes
2. Factor Productos y Servicios / Activos Virtuales
3. Factor Canales
4. Factor Transaccional
5. Factor Geográfico

Fortaleza de los Mitigantes

1. Políticas y Procedimientos PLA/FT
2. Gobierno Corporativo
3. KYC/Debida Diligencia del Cliente
4. Monitoreo, Gestión y Reporte de Operaciones Sospechosas
5. Capacitación
6. Oficial de Cumplimiento, Área de PLA/FT y Comité de PLA/FT
7. Auditoría y revisión del sistema de PLA/FT
8. Coin Risk Assessment

Riesgo Residual

Se determina equilibrando el nivel de riesgo inherente con la solidez general de los controles de gestión de riesgos.

Coin Risk Assessment

Liquidez

Equipo detrás

Seguridad

Antigüedad

Proof of Reserve

Reputación

Auditorías financieras

Trazabilidad

Conoce y monitorea en tiempo real el riesgo de tus terceras partes.

Enfoque holístico del riesgo

Optimiza tu tiempo y tus recursos

Monitoreo Transaccional (KYT).

Herramientas para el monitoreo de transacciones en Activos Virtuales

Chainalysis

CIPHERTRACE

TRM

ELLIPTIC

Blacklist de direcciones

El GAFI estipula que, si un VASP descubre direcciones de AV con las que ha decidido no establecer o continuar relaciones comerciales o realizar transacciones debido a sospechas de LA/FT, el VASP debería considerar la posibilidad de poner a disposición su lista de "direcciones de billetera en la lista negra", sujeta a las leyes de la jurisdicción del VASP.

Un VASP debería cotejar las direcciones de sus clientes y contrapartes con dichas direcciones de la lista negra disponibles como parte de su supervisión continua.

Un VASP debe hacer su propia evaluación basada en el riesgo y determinar si se justifican acciones adicionales de mitigación o prevención si hay un resultado positivo.

Gracias

Delfina Chain

delfina@chaindots.com