C E T I D

Centro de Estudios Tecnológicos en Informática y Derecho

NEWSLETTER · LAS CINCO CURVAS CONVERGENTES

Edición 10-05 · Quito, 30 de octubre de 2026

Seis mil millones de dólares en veinte minutos

El hackeo a Binance leído desde las cinco curvas convergentes: ciberseguridad, protección de datos, gobernanza de la inteligencia artificial, propiedad intelectual y criptoactivos

Dr. Juan José Páez Rivadeneira
Director del CETID

En síntesis

El 29 de octubre de 2026 un atacante sustrajo cerca de 6360 millones de dólares de las billeteras de Binance, la mayor plataforma de intercambio de criptoactivos del mundo. Es el mayor robo de activos digitales registrado. Esta edición sostiene una tesis: el incidente no pertenece a una sola rama del derecho. Activa a la vez las cinco curvas convergentes y deja a la vista una brecha del ordenamiento ecuatoriano, que vigila a los proveedores de activos virtuales para prevenir el lavado de activos, pero no los regula para proteger a sus clientes.

1. Los hechos verificados

La reconstrucción que sigue se limita a lo que confirman al menos dos fuentes independientes a las 10:00 (hora de Ecuador) del 30 de octubre de 2026. Las cifras son provisionales y pueden variar.

- **Cuándo y cuánto.** Según TRM Labs, la salida de fondos empezó el 29 de octubre a las 20:05 UTC (15:05 en Ecuador). La mayor parte ocurrió en unos veinte minutos y afectó billeteras en diez cadenas de bloques. TRM cuantifica lo sustraído en 6360 millones de dólares; Binance lo estima en 6300 millones (Tomasicchio, 2026; Al Jazeera, 2026).
- **Respuesta inmediata.** Binance suspendió depósitos y retiros y anunció que cubrirá todas las pérdidas con fondos propios y con su fondo de protección para usuarios (SAFU). Con apoyo de Tether, Circle, World Liberty Financial y el custodio BitGo, se congelaron cerca de 3000 millones; unos 3300 millones seguían sin congelar en los últimos reportes (Forbes, 2026; Newsy Today, 2026).
- **Vector de ataque.** La investigación preliminar de Binance apunta a la computadora portátil comprometida de un ingeniero de DevOps. Ese acceso habría permitido entrar a un contenedor de servicio y enviar órdenes de retiro no autorizadas. Binance afirma que no halló indicios de filtración de claves privadas y, en una actualización posterior, informó de otros puntos de intrusión (SecurityWeek, 2026; Hackread, 2026).
- **Autoría.** TRM Labs atribuye el ataque, con alta confianza, a TraderTraitor, unidad vinculada a Corea del Norte. Chainalysis considera probable esa autoría. Binance no ha confirmado la atribución (SecurityWeek, 2026).
- **Contexto.** El récord anterior era el robo de 1500 millones de dólares a Bybit en febrero de 2025, que el FBI atribuyó a la misma unidad (Al Jazeera, 2026).

Una advertencia metodológica: durante las primeras horas circularon cifras de 2000, 3500, 5700 y hasta 8900 millones. La cifra con mejor respaldo es la de Binance y TRM. Además, 3000 millones *congelados* no equivalen a 3000 millones *recuperados*.

2. Tesis: un incidente, cinco curvas

El marco de las cinco curvas convergentes parte de una premisa: el riesgo tecnológico ya no se deja encerrar en compartimentos normativos. Ciberseguridad, protección de datos, gobernanza de la inteligencia artificial, propiedad intelectual y criptoactivos crecen a ritmos distintos, pero se cruzan en los incidentes reales. El caso Binance es un caso testigo: un acceso indebido a un equipo de trabajo (ciberseguridad) movió activos cuya naturaleza jurídica sigue en debate (criptoactivos), dentro de una plataforma que custodia datos de identificación de millones de clientes (protección de datos), con una autoría inferida por sistemas analíticos (inteligencia artificial) y con un punto de entrada en el conocimiento técnico interno de la empresa (propiedad intelectual).

3. Primera curva: ciberseguridad y evidencia digital

3.1. El eslabón débil no fue la criptografía

Si se confirma la versión preliminar, el atacante no rompió la criptografía ni robó las claves privadas. Usó los sistemas autorizados para mover fondos. La consecuencia jurídica es relevante: la diligencia exigible a un custodio de criptoactivos no se agota en guardar claves. Comprende la gestión de accesos privilegiados, la seguridad de los equipos del personal técnico y la segmentación de la infraestructura de firma.

3.2. El marco ecuatoriano de ciberseguridad

La Ley Orgánica para el Fortalecimiento de la Ciberseguridad (LOFC), publicada en el Registro Oficial 290, quinto suplemento, de 22 de mayo de 2026, reformó la Ley Orgánica para la Transformación Digital y Audiovisual. Entre sus reglas destacan tres:

- la obligación de notificar incidentes de ciberseguridad relevantes en un plazo máximo de 72 horas desde su detección (artículo 20-G incorporado);
- la creación del CSIRT Nacional como instancia técnica de respuesta; y,
- la regla de que esa notificación no sustituye la obligación de denunciar los hechos que constituyan delitos de acción pública (Corral Rosales, 2026).

Queda abierta una pregunta: si una plataforma extranjera que presta servicios a residentes en Ecuador, sin licencia local, es «prestador de servicios digitales» para efectos de la LOFC. La respuesta definirá si el Estado puede exigirle información sobre incidentes que afecten a usuarios ecuatorianos.

3.3. Tipicidad penal

Con el Código Orgánico Integral Penal (COIP), los hechos encajarían, en principio, en el acceso no consentido a un sistema informático (artículo 234), el ataque a la integridad de sistemas informáticos (artículo 232) y la apropiación fraudulenta por medios electrónicos (artículo 190). La conversión y ocultamiento posterior de los fondos remite al lavado de activos (artículo 317). La competencia de los jueces ecuatorianos dependería de la existencia de víctimas o efectos en el país.

3.4. Cooperación internacional y prueba

Ecuador depositó el instrumento de adhesión al Convenio sobre la Ciberdelincuencia (Convenio de Budapest) el 12 de diciembre de 2024 y es Estado parte desde el 1 de abril de 2025. Designó a la Fiscalía General del Estado como punto de contacto 24/7 (Consejo de Europa, 2024; OMPI, s. f.). El

Convenio ofrece herramientas de uso inmediato: la conservación rápida de datos informáticos (artículos 16 y 29) y la red 24/7 (artículo 35).

La cadena de bloques es un registro público: cualquiera puede verificar las transacciones. Lo que no muestra es quién está detrás de cada dirección. La atribución exige evidencia fuera de la cadena, y los informes de empresas de análisis deben ingresar al proceso con su metodología, bajo las reglas de cadena de custodia (artículo 456 del COIP) y de contenido digital (artículo 500 del COIP).

4. Segunda curva: protección de datos personales

Las plataformas de intercambio figuran entre los mayores repositorios privados de datos de identificación: documentos, biometría, domicilio y patrimonio de sus clientes. La información pública disponible no permite saber si el atacante accedió a datos personales. Si lo hizo y hay titulares residentes en Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPDP) impone obligaciones precisas.

- **Notificación a la autoridad.** El artículo 43 de la LOPDP, reformado por la LOFC, exige notificar la vulneración tan pronto sea posible y, a más tardar, en el término de cinco días. La notificación se dirige a la Superintendencia de Protección de Datos Personales (SPDP), al regulador sectorial y, para coordinación técnica, al CSIRT (Meythaler & Zambrano, 2026).
- **Cadena responsable–encargado.** La norma técnica expedida mediante Resolución SPDP-SPD-2026-0040-R (septiembre de 2026) fija en dos días el plazo del encargado para avisar al responsable (Écija, 2026).
- **Comunicación a los titulares**, cuando la vulneración entrañe riesgo para sus derechos.

El caso revela además una tensión de fondo. La regla de viaje del Grupo de Acción Financiera Internacional (GAFI), recogida en el artículo 52 de la ley antilavado ecuatoriana, obliga a que los datos del ordenante y del beneficiario acompañen cada transferencia de activos virtuales. La prevención del lavado exige más datos; la minimización de datos exige menos. Cada dato adicional amplía la superficie de ataque. La solución no es elegir uno de los dos fines, sino diseñar la seguridad desde el origen para que ambos convivan.

5. Tercera curva: gobernanza de la inteligencia artificial

No existe evidencia pública de que el atacante empleara inteligencia artificial. La curva aparece por otra vía: la atribución. En menos de 24 horas, dos empresas privadas señalaron a una unidad estatal extranjera mediante análisis automatizado de patrones en la cadena de bloques y de inteligencia externa. Es una inferencia probabilística, valiosa para la investigación, pero que no equivale a prueba de autoría.

Para el proceso penal, esto plantea la misma exigencia que el CETID ha sostenido respecto de todo sistema algorítmico con efectos jurídicos: explicabilidad. Un juez debe poder conocer qué heurísticas agruparon las direcciones, con qué margen de error y qué datos alimentaron el modelo. El GAFI, en su actualización de julio de 2026 sobre activos virtuales, ya incorpora el uso de inteligencia artificial en los delitos con activos virtuales entre los riesgos emergentes (GAFI, 2026; 21 Analytics, 2026).

6. Cuarta curva: propiedad intelectual

Es la curva menos visible del caso y, como hemos advertido en otras ediciones, la menos desarrollada doctrinalmente. Aun así, ofrece tres lecturas:

- **El código no es el token.** En *Van Loon v. Department of the Treasury* (2024), el Quinto Circuito de Estados Unidos resolvió que los contratos inteligentes inmutables de Tornado

Cash no son «propiedad» a efectos de las sanciones, porque nadie puede poseerlos ni controlarlos. El derecho empieza a distinguir entre el activo (apropiable) y la infraestructura de código que lo mueve (a veces inapropiable).

- **El activo atacado fue el conocimiento interno.** El atacante no necesitó las claves: le bastó conocer y usar la arquitectura interna de firma y retiro. Esa información técnica es, en sí misma, un secreto empresarial cuya protección jurídica y técnica forma parte de la diligencia del custodio.
- **La cadena de suministro de software.** La unidad señalada es conocida por atacar a desarrolladores mediante falsas entrevistas de trabajo y paquetes de software maliciosos (daily.dev, 2026). Las licencias y dependencias de código abierto son también un problema de responsabilidad.

7. Quinta curva: criptoactivos

7.1. ¿De quién son los activos en una plataforma?

La jurisprudencia comparada responde en dos tiempos. Primero, los criptoactivos son propiedad. En *AA v Persons Unknown* [2019] EWHC 3556 (Comm), el juez Bryan concedió un mandamiento cautelar sobre bitcoins pagados como rescate y los reconoció como propiedad. En *Ruscoe v Cryptopia Ltd (in liq)* [2020] NZHC 728, el juez Gendall (Nueva Zelanda) resolvió que la plataforma, tras ser hackeada, mantenía los criptoactivos en fideicomiso para sus clientes. El Reino Unido codificó esta línea con la Property (Digital Assets etc) Act 2025, vigente desde el 2 de diciembre de 2025, que admite una tercera categoría de bienes muebles (Law Commission, 2025).

Segundo, la propiedad no decide por sí sola la suerte del cliente: deciden los términos de uso. En *In re Celsius Network LLC* (Bankr. S.D.N.Y., 4 de enero de 2023), el juez Glenn concluyó que los términos aceptados por los clientes transferían a la plataforma la titularidad de los activos depositados en las cuentas «Earn». Esos clientes quedaron como acreedores quirografarios. La lección para los usuarios ecuatorianos de Binance es directa: su posición jurídica ante una pérdida depende del contrato que aceptaron con un clic.

7.2. El congelamiento privado: eficaz y sin juez

En pocas horas, Tether y Circle inmovilizaron más de 2300 millones de dólares en sus monedas estables mediante listas de bloqueo (Forbes, 2026). Funcionó como una medida cautelar sin proceso, dictada por un emisor privado sobre cualquier dirección. Es eficaz contra el delito, pero plantea una pregunta de garantías: el mismo poder puede congelar los fondos de un tercero de buena fe.

El contraste con Ecuador es ilustrativo. El artículo 17.3 de la ley antilavado, incorporado en agosto de 2025, permite a la Unidad de Análisis Financiero y Económico (UAFE) inmovilizar fondos de forma excepcional. La medida debe ejecutarse en 72 horas, dura hasta ocho días y requiere ratificación judicial. Pero se limita a fondos «en el Sistema Financiero Nacional». No alcanza a monedas estables emitidas en el exterior ni a billeteras en plataformas extranjeras.

7.3. La responsabilidad del custodio

La Unión Europea resolvió esta cuestión por ley. El Reglamento (UE) 2023/1114 (MiCA) obliga a los proveedores a salvaguardar los criptoactivos de los clientes y a impedir su uso por cuenta propia (artículo 70). Además, los hace responsables ante sus clientes por la pérdida de criptoactivos o de los medios de acceso derivada de un incidente que les sea atribuible (artículo 75). En el modelo europeo, cubrir la pérdida es un deber legal; en el caso Binance, por ahora, es una promesa comercial.

7.4. Ecuador: vigilancia antilavado sin régimen de protección

El estado del derecho ecuatoriano puede resumirse en cuatro datos:

1. El Banco Central del Ecuador sostiene que los criptoactivos no son moneda de curso legal ni medio de pago autorizado.
2. La Ley Orgánica de Prevención, Detección y Combate del Delito de Lavado de Activos y de la Financiación de Otros Delitos (Registro Oficial 610, cuarto suplemento, 29 de julio de 2024) define el activo virtual y al proveedor de servicios de activos virtuales (artículo 4, literales a y z). Los incluye como sujetos obligados (artículos 26 y 31), les impone la regla de viaje (artículo 52) y los somete a la supervisión de la Superintendencia de Bancos (artículo 65, numeral 1, literal f).
3. El Decreto-Ley 477, que había incorporado al Código Orgánico Monetario y Financiero un régimen de licencias para proveedores de activos virtuales (artículos 99.1 y 99.2), fue declarado inconstitucional por la forma, con efectos retroactivos, en la sentencia 94-24-IN/25 de la Corte Constitucional, de 23 de enero de 2025. Ese régimen desapareció del ordenamiento.
4. El 19 de octubre de 2026, el Consejo de Administración Legislativa calificó el Proyecto de Ley Orgánica de Activos Virtuales, presentado por la asambleísta Inés Alarcón, y lo remitió a la Comisión de Seguridad Integral. Según la información oficial, propone un registro obligatorio, autorizaciones para actividades de mayor riesgo, debida diligencia, trazabilidad y extinción de dominio (Jaramillo, 2026).

El proyecto, tal como se ha descrito públicamente, privilegia el control y la seguridad. El caso Binance demuestra que falta la otra mitad: reglas de segregación patrimonial, custodia y responsabilidad que protejan al cliente cuando el custodio falla. Su texto completo aún no es público, por lo que esta observación debe contrastarse cuando se conozca.

8. La dimensión geopolítica

Si la atribución se confirma, el caso deja de ser un delito patrimonial común. El Equipo Multilateral de Monitoreo de Sanciones (MSMT), integrado por once Estados, informó en octubre de 2025 que Corea del Norte sustrajo al menos 1190 millones de dólares en criptoactivos en 2024 y 1650 millones entre enero y septiembre de 2025. Según ese informe, esos fondos sirven para financiar sus programas de armas. El MSMT nació después de que el veto de Rusia disolviera, en abril de 2024, el panel de expertos del Consejo de Seguridad de las Naciones Unidas (World ECR, 2025).

Para los sujetos obligados ecuatorianos, esto tiene consecuencias concretas. La ley antilavado incluye la financiación de la proliferación de armas de destrucción masiva entre los riesgos que deben gestionar (artículos 4, literal p, y 37) y les ordena monitorear las listas del Consejo de Seguridad (artículo 55). Un proveedor local que reciba una fracción de los fondos robados debe reportar la operación sospechosa a la UAFE.

9. Matriz de convergencia

Curva	**Pregunta que abre el caso**	**Referencia normativa o jurisprudencial**
Ciberseguridad	¿Debe notificar en Ecuador una plataforma extranjera sin licencia local?	LOFC, art. 20-G; Convenio de Budapest, arts. 16, 29 y 35; COIP, arts. 190, 232 y 234
Protección de datos	¿Hubo acceso a datos de clientes y a quién se notifica?	LOPDP, art. 43 (reformado por la LOFC); Res. SPDP-SPD-2026-0040-R

Curva	Pregunta que abre el caso	Referencia normativa o jurisprudencial
Inteligencia artificial	¿Qué valor probatorio tiene una atribución algorítmica?	Principio de explicabilidad; COIP, arts. 456 y 500
Propiedad intelectual	¿Es el código propiedad? ¿Se protegió el secreto técnico?	Van Loon v. Department of the Treasury (5th Cir. 2024)
Criptoactivos	¿El cliente es propietario o acreedor? ¿Quién responde?	AA v Persons Unknown; Ruscoe v Cryptopia; In re Celsius; MiCA, arts. 70 y 75; CCE 94-24-IN/25

10. Cinco propuestas de lege ferenda para Ecuador

1. **Régimen de custodia.** Incorporar al proyecto de ley la segregación de los activos de los clientes, la prohibición de usarlos por cuenta propia y la responsabilidad del custodio por pérdidas atribuibles a incidentes, en la línea de los artículos 70 y 75 de MiCA.
2. **Seguridad operativa exigible.** Exigir a los proveedores de servicios de activos virtuales controles de accesos privilegiados, seguridad de equipos del personal técnico y pruebas periódicas, articulados con la LOFC.
3. **Ventanilla única de notificación.** Coordinar en un solo canal las notificaciones de un incidente con criptoactivos: 72 horas (LOFC), cinco días (LOPDP) y el reporte de operación sospechosa a la UAFE.
4. **Medidas cautelares con garantías.** Regular el congelamiento de criptoactivos y la cooperación con emisores extranjeros de monedas estables, con control judicial y protección del tercero de buena fe.
5. **Prueba digital en cadena de bloques.** Adoptar protocolos de análisis en cadena admisibles en juicio, acreditar peritos y fijar reglas de custodia para billeteras y claves incautadas.

11. Reflexión final

El aforismo *nemo plus iuris ad alium transferre potest quam ipse habet* recuerda que nadie puede transmitir a otro más derecho del que tiene. El ladrón de criptoactivos no adquiere título y no puede transmitirlo. Pero la cadena de bloques no conoce títulos, solo firmas válidas. Los congelamientos de Tether y Circle son, quizá, la primera traducción técnica de ese viejo principio. Al derecho le corresponde decidir quién puede aplicarlo, con qué límites y ante qué juez.

Nota de verificación

Los hechos se verificaron con fuentes periodísticas y técnicas consultadas el 30 de octubre de 2026 por la mañana (hora de Ecuador). Las cifras del incidente, el vector de ataque y la atribución son preliminares. La normativa ecuatoriana se cotejó con textos oficiales y compilaciones actualizadas; el texto completo del Proyecto de Ley Orgánica de Activos Virtuales no estaba disponible al cierre de esta edición.

Referencias

Normativa

Código Orgánico Integral Penal. Registro Oficial 180, suplemento, 10 de febrero de 2014 (con sus reformas).

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia* (STE n.º 185). Budapest.

Ley Orgánica de Prevención, Detección y Combate del Delito de Lavado de Activos y de la Financiación de Otros Delitos. Registro Oficial 610, cuarto suplemento, 29 de julio de 2024 (última reforma: 3 de octubre de 2025).

Ley Orgánica de Protección de Datos Personales. Registro Oficial 459, suplemento, 26 de mayo de 2021.

Ley Orgánica para el Fortalecimiento de la Ciberseguridad. Registro Oficial 290, quinto suplemento, 22 de mayo de 2026.

Property (Digital Assets etc) Act 2025 (Reino Unido).

Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, relativo a los mercados de criptoactivos (MiCA). *Diario Oficial de la Unión Europea*, L 150, 9 de junio de 2023.

Superintendencia de Protección de Datos Personales. Resolución SPDP-SPD-2026-0040-R, Norma Técnica de Notificación de Vulneraciones de Seguridad de Datos Personales (septiembre de 2026).

Jurisprudencia

AA v Persons Unknown [2019] EWHC 3556 (Comm).

Corte Constitucional del Ecuador. Sentencia 94-24-IN/25, 23 de enero de 2025.

In re Celsius Network LLC, No. 22-10964 (MG), 2023 WL 34106 (Bankr. S.D.N.Y. Jan. 4, 2023).

Ruscoe v Cryptopia Ltd (in liq) [2020] NZHC 728.

Van Loon v. Department of the Treasury, 122 F.4th 549 (5th Cir. 2024).

Doctrina e informes

21 Analytics. (2026, 20 de julio). *2026 FATF targeted update summarised: Part 1*. https://www.21analytics.co/blog/2026-fatf-targeted-update-part1/

Babie, P. T., Brown, D., Catterwell, R., y Giancaspro, M. (2020). *Cryptocurrencies as property: Ruscoe and Moore v Cryptopia Limited (In Liquidation) [2020] NZHC 728*. SSRN.

Federal Court of Australia. (2024, 21 de junio). *Is cryptocurrency property?* [Discurso del juez Jackman]. https://www.fedcourt.gov.au/digital-law-library/judges-speeches/justice-jackman/jackman-j-20240621

Fox, D., y Green, S. (Eds.). (2019). *Cryptocurrencies in public and private law*. Oxford University Press.

Grupo de Acción Financiera Internacional (GAFI). (2026). *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-updated-virtualassets-vasps-2026.html

Law Commission. (2023). *Digital assets: Final report* (Law Com No 412).

Law Commission. (2025). *The Property (Digital Assets etc) Act 2025 has received Royal Assent*. https://www.lawcom.gov.uk/the-property-digital-assets-etc-act-2025-has-received-royal-assent

Páez Rivadeneira, J. J. (2026). *Ciberseguridad: Marco jurídico, técnico y estratégico*. CETID.

UK Jurisdiction Taskforce. (2019). *Legal statement on cryptoassets and smart contracts*.

Fuentes periodísticas y técnicas

Al Jazeera. (2026, 30 de octubre). *Binance says $6.3bn stolen in biggest crypto heist in history*. https://www.aljazeera.com/economy/2026/10/30/binance-says-2-54bn-in-crypto-funds-frozen-amid-potential-security-issue

CoinDesk. (2026, 29 de octubre). *Binance pierde 5.7 mil millones de dólares en el mayor hackeo de criptomonedas hasta la fecha*. https://www.coindesk.com/es/business/2026/10/29/potential-multi-billion-binance-hack-hitting-crypto-markets

Consejo de Europa. (2024, 12 de diciembre). *Convention on Cybercrime: Ecuador becomes the 77th Party*. https://www.coe.int/en/web/cybercrime/-/convention-on-cybercrime-ecuador-becomes-the-77th-party-and-peru-signs-the-second-protocol-on-electronic-evidence

Corral Rosales. (2026). *Ley Orgánica para el Fortalecimiento de la Ciberseguridad: publicación en el Registro Oficial y obligaciones para el sector privado*. https://corralrosales.com/ley-organica-para-el-fortalecimiento-de-la-ciberseguridad-publicacion-en-el-registro-oficial-y-obligaciones-para-el-sector-privado/

daily.dev. (2026). *Binance hack: How a developer laptop can put $6.3B in play*. https://daily.dev/posts/binance-hack-how-a-developer-laptop-can-put-6-3b-in-play-7cprtijyg

Écija. (2026, 24 de septiembre). *Nueva Norma Técnica de Notificación de Vulneraciones de Seguridad de Datos Personales*. https://www.ecija.com/actualidad-insights/nueva-norma-tecnica-de-notificacion-de-vulneraciones-de-seguridad-de-datos-personales/

Forbes. (2026, 30 de octubre). *Binance hit by $6.3 billion hack in what may be crypto's biggest theft*. https://www.forbes.com/sites/jonmarkman/2026/10/30/binance-hit-by-63-billion-hack-in-what-may-be-cryptos-biggest-theft/

Hackread. (2026). *Binance probes DevOps engineer's hacked laptop after $6.3B theft*. https://hackread.com/binance-devops-engineer-hacked-laptop-billion-theft/

Jaramillo, F. (2026, 23 de octubre). Ecuador inicia el trámite de una ley de activos virtuales que exigiría registro a exchanges y custodios. *Criptoinforme*. https://criptoinforme.com/legal/ley-activos-virtuales-ecuador-exchanges-registro/

Meythaler & Zambrano Abogados. (2026). *Ley de Ciberseguridad en Ecuador: obligaciones y sanciones*. https://www.meythalerzambranoabogados.com/post/ley-ciberseguridad-ecuador-lofc

Newsy Today. (2026, 30 de octubre). *$6.3B US crypto stolen in record Binance hack*. https://www.newsy-today.com/6-3b-us-crypto-stolen-in-record-binance-hack/

OMPI. (s. f.). *WIPO Lex: Convention on Cybercrime, Ecuador*. https://www.wipo.int/wipolex/en/treaties/parties/remarks/EC/952

SecurityWeek. (2026). *$6 billion Binance hack bears hallmarks of North Korea's TraderTraitor*. https://www.securityweek.com/6-billion-binance-hack-bears-hallmarks-of-north-koreas-tradertraitor/

Tomasicchio, A. (2026, 30 de octubre). TRM afirma que el hackeo de criptomonedas a Binance robó 6,36 mil millones de dólares en 10 cadenas. *The Cryptonomist*. https://es.cryptonomist.ch/2026/10/30/trm-afirma-que-el-hackeo-de-criptomonedas-a-binance-robo-636-mil-millones-de-dolares-en-10-cadenas-en-su-mayoria-en-20-minutos/

World ECR. (2025, 30 de octubre). *North Korea stole $2.84b in crypto over 21 months, allied monitoring team reports*. https://www.worldecr.com/news/north-korea-stole-2-84b-in-crypto-over-21-months-allied-monitoring-team-reports/

CETID · Centro de Estudios Tecnológicos en Informática y Derecho

www.cetid.abogados.ec · info@cetid.abogados.ec · WhatsApp 096 276 0302 · Quito, Ecuador

Este contenido es informativo y académico. No constituye asesoría jurídica ni recomendación de inversión.