Cronología de un hackeo histórico: paso a paso, qué se sabe del caso Binance, el mayor robo de la historia cripto

infobae.com/economia/2026/10/31/cronologia-de-un-hackeo-historico-paso-a-paso-que-se-sabe-del-caso-binance-el-mayor-robo-de-la-historia-cripto

Sebastián Catalano October 31, 2026



El logo de Binance (REUTERS/Dado Ruvic/Illustration)

Fue un ataque quirúrgico, rápido y, según los analistas, preparado con días de anticipación. En una ventana de unos 20 minutos del jueves por la tarde (hora argentina), un atacante vació billeteras de Binance en diez blockchains. Reuters informó que los hackers robaron USD 6.300 millones al mayor *exchange* del mundo, en un golpe que los analistas atribuyen a Corea del Norte y que podría ser el mayor robo financiero de todos los tiempos. CNBC lo calificó como el mayor hackeo cripto registrado.

La escala no tiene precedentes. TRM Labs calculó que equivale a unas cuatro veces el hackeo a Bybit de febrero de 2025, hasta ahora el récord, con USD 1.500 millones. Elliptic fue más lejos: **dijo que el incidente es casi con certeza el mayor robo conocido de cualquier tipo**.

El golpe cae sobre una compañía con 335 millones de usuarios registrados y unos USD 162.800 millones en custodia a fines de 2025. Binance dice que los fondos de los clientes están a salvo y que absorberá las pérdidas. El desenlace depende de que cumpla esa promesa, de que logre rastrear lo que falta y de cuánto tarde en reabrir los retiros.

Cronología

- **La advertencia.** El martes pasado, Binance comunicó que había bloqueado, durante la semana previa, múltiples intentos de ciberataque vinculados a actores norcoreanos, sin pérdidas de activos.
- **Arranca la preparación.** Un día después, según TRM, la billetera operadora del atacante recibió tres retiros pequeños de Tornado Cash, unas 36 horas antes del robo. Ese patrón coincide con golpes previos atribuidos a Corea del Norte, entre ellos Bybit y KelpDAO.
- **Empieza el vaciamiento.** El jueves, cerca de las 17 horas de Argentina, cinco billeteras de Binance en XRP Ledger enviaron 233 millones de XRP a una dirección del atacante. A las 20:20 siguieron Bitcoin (18.270 BTC) y Ethereum, donde el atacante usó 50 autorizaciones EIP-7702 firmadas de antemano para convertir una billetera caliente en un “barredor” bajo su control.
- **Congelan los emisores.** Tether congeló fondos a las 21:01, Circle a las 21:04, Ripple a las 22:01 y World Liberty Financial a las 22:10. Reuters precisó que Tether congeló casi USD 1.570 millones y Circle más de USD 800 millones.



Changpeng Zhao, fundador y exCEO de exchange cripto (REUTERS/Tyrone Siu)

- **Noche del jueves: la noticia se hace pública.** Bloomberg informó que Binance suspendió retiros y prometió cubrir las pérdidas, con unos USD 3.000 millones congelados según una publicación de la empresa en X. Bloomberg Línea había reportado antes que Binance cubriría todas las pérdidas y que la cifra congelada entonces era de USD 2.540 millones. Changpeng Zhao, cofundador y ex CEO, escribió en X que “sí parece un hackeo”.
- **Segunda ola.** Billeteras de Binance en Avalanche y Polygon también enviaron fondos al atacante.
- **Jueves a la noche: la hipótesis oficial.** Binance dijo en X que la investigación inicial apuntaba a la laptop comprometida de un ingeniero de DevOps y que no encontró evidencia de filtración de claves privadas. La empresa estimó el impacto en USD 6.300 millones.
- **Viernes a la mañana: se complica el cuadro.** Reuters resumió el mensaje de Richard Teng, co-CEO: fue un ataque complejo, no de una sola persona, con una laptop comprometida y software malicioso que borraba rastros sobre la marcha. Los atacantes manipularon un sistema de aprobación de transacciones para mover dinero fuera de la billetera caliente sin pasar por los controles normales.
- **Llega la atribución.** TRM Labs y Chainalysis atribuyeron el hackeo a TraderTraitor, un grupo norcoreano respaldado por el Estado. El FBI había identificado al mismo grupo como responsable del robo a Bybit. Forbes, citando al WSJ, agregó que otra firma de inteligencia cripto, Pangolin Intelligence, llegó a la misma conclusión. Corea del Norte suele negar este tipo de acusaciones y no respondió a Reuters.
- **Intervienen las autoridades.** El viernes al mediodía, Reuters informó que Binance trabaja con el FBI y el Servicio Secreto, y que el regulador de Abu Dabi que emitió su licencia principal sigue el caso. El presidente de la CFTC, Michael Selig, dijo en CNBC que la brecha prueba la necesidad de regular el mercado.
- **El plan de reposición.** Binance apartó más de USD 6.340 millones, de los cuales USD 5.000 millones ya están en las mismas criptomonedas afectadas, y comprará el resto en mercados y operaciones OTC. El WSJ indicó que el fondo SAFU tenía USD 1.230 millones en Bitcoin el jueves, menos que el total robado. Teng prometió una prueba de reservas el lunes y retiros antes del domingo. Yi He, por su parte, dijo en X que los USD 3.000 millones congelados representan apenas el 2% de los activos de usuarios y reservas públicas.
- **Mercados.** Reuters registró que el bitcoin tocó un mínimo de seis semanas en USD 76.368 y que el BNB cayó 6,74% en 24 horas. CNBC consignó que el bitcoin llegó a caer más de 4% el viernes.
- **Qué falta.** TRM estima que el atacante retiene unos USD 2.400 millones, entre ellos más de 420.000 ETH y 18.270 BTC. Ari Redbord, de TRM, describió a CNBC una carrera contra el tiempo para recuperar los fondos. La CEO de Bitget, Gracy Chen, dijo a CNBC que no espera recuperar mucho. Reuters aclaró que Binance no informó el estado de los USD 3.300 millones restantes.
- **Viernes 30/10, tarde: la reposición, al 80%.** En su segundo comunicado de seguridad, Binance dijo que ya cubrió aproximadamente el 80% del monto afectado. Apartó más de USD 6.340

millones, de los cuales USD 5.000 millones están en los mismos activos robados (USDC, USDT, BTC, ETH, BNB). El 20% restante lo compra en el mercado y en operaciones OTC. Los depósitos siguen operativos. Los retiros volverían en unas 34 horas, de forma gradual y sujetos a las verificaciones de seguridad.

- **Viernes: la investigación suma frentes.** Binance admitió que la hipótesis de la laptop comprometida quedó incompleta: la investigación posterior encontró “puntos adicionales de vulneración”. Dijo que hasta ahora no halló evidencia de que se hayan filtrado las claves privadas de las billeteras. Prometió hallazgos técnicos en unas 48 horas y un informe completo. Planea una primera instantánea de *Proof of Reserves* en 12 horas, con resultados el lunes 2 de noviembre.