Corea del Norte considera innecesario dialogar con EEUU tras las acusaciones sobre el robo a Binance

corea del Norte afirmó este miércoles que «**no tiene necesidad**» de hablar con Washington tras las acusaciones del FBI de su implicación en el robo a la plataforma de criptomonedas Binance, en medio de las intenciones del presidente estadounidense, Donald Trump, de reunirse este año con el líder norcoreano, Kim Jong-un.

«**Es nuestra postura clara que no tenemos necesidad alguna de sentarnos cara a cara con personas tan poco fiables y hostiles**», dijo Kim Yo-jong, la influyente hermana del mandatario norcoreano, en referencia a Estados Unidos, según un comunicado difundido por la agencia estatal KCNA.

Kim también consideró que las acusaciones relacionadas con el robo a Binance forman parte de la política hostil de Washington hacia Pionyang, en lugar de constituir un episodio aislado, y acusó a Estados Unidos de intentar sacar provecho político y estratégico del caso.

No obstante, reconoció que el diálogo es una de las vías para alcanzar la paz, pero matizó que recurrir a él no necesariamente responde a los intereses nacionales de Corea del Norte.

Bajas expectativas de una reunión entre Trump y Kim Jong-un

La postura de Pionyang enfría las expectativas de un encuentro entre Trump y Kim Jong-un este año, incluida la posibilidad de que ambos líderes se reúnan al margen de la visita del mandatario estadounidense a Shenzhen, China, con motivo de la cumbre del Foro de Cooperación Económica Asia-Pacífico (APEC) del 18 y 19 de noviembre.

Apenas en la víspera, la hermana del líder norcoreano tachó de «**absurda**» la acusación del FBI sobre una supuesta implicación norcoreana en el robo histórico de datos a Binance y de que insinuara que la propia Administración de Trump podría beneficiarse de la recuperación de los activos sustraídos.

También este miércoles, Corea del Norte lanzó varios misiles desde la zona nororiental de Sondok, hacia el mar de Japón (llamado mar del Este en las dos Coreas).

Binance explica cómo comenzó el ciberataque

Por su parte, la plataforma de intercambio de criptomonedas Binance reveló que el ciberataque sufrido recientemente, con un impacto estimado en 6 mil 340 millones de dólares y atribuido por EEUU a Corea del Norte, comenzó con una operación de infiltración mediante falsas entrevistas de trabajo.

En un informe preliminar publicado en las últimas horas en la red social X, la compañía explicó que los atacantes emplearon técnicas de «**ingeniería social**», herramientas de inteligencia artificial y mecanismos avanzados de autorización de transacciones para sustraer los activos.

«**No fue una única brecha aislada ni un simple incidente de suplantación de identidad**», señaló Binance, que describió una operación «**sofisticada**» desarrollada en varias etapas.

Según su reconstrucción, en septiembre un ingeniero recibió una oferta laboral ficticia y participó en dos entrevistas, tras las cuales descargó en su ordenador de trabajo un supuesto ejercicio técnico que contenía código malicioso.

Posteriormente, los atacantes utilizaron una herramienta interna de inteligencia artificial para comprometer otros equipos y obtener credenciales que les permitieron acceder al sistema de autorización de operaciones.

El 29 de octubre ejecutaron transferencias no autorizadas de diversas criptomonedas, entre ellas bitcoines, XRP y activos de las redes Solana y Ethereum.

Binance reconoció que la suspensión de los retiros no bastó para detener inmediatamente el robo, debido a autorizaciones maliciosas que permitían mover fondos al margen de su «**infraestructura habitual**».

«**Esto no debería haber ocurrido y pedimos disculpas por la preocupación, las interrupciones y la incertidumbre causadas**», afirmó la compañía.

La plataforma aseguró que ha repuesto el 98 % de los activos afectados y reservado fondos suficientes para cubrir las pérdidas, mientras que unos 2 mil 850 millones de dólares permanecen congelados o han sido interceptados.

Asimismo, anunció una revisión independiente de sus sistemas de seguridad y mayores inversiones en herramientas de detección basadas en inteligencia artificial.

EFE