



ACTA DE SORTEO CERTIFICADO

SORTIVEN V1.4 — Sistema de Sorteo Auditable · Aleatoriedad Verificable (Provably Fair)

1. Identificación del Sorteo

ID del sorteo	52d425ee-ab9d-48ac-b818-8207a01d895d
Nombre	Sorteo 2 test
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-07-13T15:25:47.101432+00:00
Ejecutado	2026-07-13T15:25:59.084241+00:00
Revelado	2026-07-13T15:26:13.342721+00:00

2. Resultado Oficial

09 · Águila

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	e9c86853436f8e8a1133d01656a821afa4367646f4ad01e4585894893c516cf8
Semilla del cliente (client seed)	492003f4a8465f97
Nonce	1
Semilla del servidor (revelada)	edad839aa2186d296a89ee2797be2454624b970fba7324221bbc9e39efe93f58

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	6
Hash anterior (prev_hash)	a1dcca9e8876380d28246b3383c494f7841e0c8bb95b010654d2da4ce1620118
Hash del registro (record_hash)	bf3e8f0ebbe9315fd5c05878d10d72125e790468ebf32f434e9c1aa8c8085cf3

5. Cómo Verificar este Sorteo

Cualquier persona puede verificar la integridad de este sorteo: (1) Confirme que SHA-256 de la **semilla del servidor revelada** es igual al **compromiso** publicado antes del sorteo. (2) Recompute el resultado con (semilla servidor, semilla cliente, nonce) usando el algoritmo público **HMAC-SHA256** con muestreo por rechazo. (3) Verifique el **record_hash** recalculando SHA-256(prev_hash + datos canónicos). El portal público de verificación realiza estos pasos automáticamente.