SORTIVEN
Sorteador Integral

ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	c786d241-7b91-4c08-8bf3-7f81219b60a9
Nombre	ZooloFalcón Venezuela — 22/10/2026 20:10
Tipo de juego	ZooloFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T20:10:49.024467+00:00
Ejecutado	2026-10-22T20:10:54.162350+00:00
Revelado	2026-10-22T20:10:59.167071+00:00

2. Resultado Oficial

44 · Chigüire

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`ca062402c9e609b01752accc43cc73718b6a9c1e9feec98dbaae79c06b027f53`
Semilla del cliente (client seed)	`d10290910005e536`
Nonce	1
Semilla del servidor (revelada)	`dcd4a65510c0967bf06175fd9e8e6378fec8299be28c70e9c3a0ab5abff50ecd`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	86
Hash anterior (prev_hash)	`4a8802e9b7172d38962444c1070b0914c27782f1cc287d85fc616d3a69f22b2c`
Hash del registro (record_hash)	`48485d2a28f97e346105cea179859406dd7fd0789889615452987c87d2b49911`

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.