



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	1bccd6b6-510e-4cf3-bb3d-7c8fa3ded9af
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 006
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:04Z
Ejecutado	2026-08-25T05:38:04Z
Revelado	2026-08-25T05:38:04Z

2. Resultado Oficial

44 · Chigüire

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	30cff1cc6f42f0c5b6ce7a69f877c6cdab26b836b815cbd6eeaac1bdd4fef9a6
Semilla del cliente (client seed)	sencamer-demo-animalitos-006
Nonce	6
Semilla del servidor (revelada)	2cab78ddef6ca0805f60979ecfe1a28b5d6109ffebd4a41ac19533c9d4af34a5

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	37
Hash anterior (prev_hash)	52aa5de2c32ca7863129f3b17d29be6aa5dd8bee019fa6f273bde08b17e3339d
Hash del registro (record_hash)	1d7c16e7591b1c6a78dd716634c5cbc898ffe5e7816dde311c3c7a4d84aa7aad

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.