

ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	354c3398-cd97-4515-810b-968d2388d677
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 002
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:02Z
Ejecutado	2026-08-25T05:38:02Z
Revelado	2026-08-25T05:38:02Z

2. Resultado Oficial

04 · Alacrán

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	b1ca4c4db030682a250d3226829622210b5855e7e39600f70920d8a7567f3c9a
Semilla del cliente (client seed)	sencamer-demo-animalitos-002
Nonce	2
Semilla del servidor (revelada)	7b0496cf287dd6e8da088327be7271ce267942f9d4b1f1b549ba9af9eecfee47

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	33
Hash anterior (prev_hash)	815d6ed5c0335b35b12e1e62049a9e8c0610b0a429a2d57d991d587dd54f7638
Hash del registro (record_hash)	f640eb9c288fd7237716b161a288c0d1b44ef7bfdd13613f1adf1cf670f891d4

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.