

ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	f4bbec14-190c-4693-ab13-2ea9590714ad
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 017
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:09Z
Ejecutado	2026-08-25T05:38:09Z
Revelado	2026-08-25T05:38:09Z

2. Resultado Oficial

04 · Alacrán

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	826f534c147e217377c200122fb56ceef303a259b7f229ce239035010e2f8bdd
Semilla del cliente (client seed)	sencamer-demo-animalitos-017
Nonce	17
Semilla del servidor (revelada)	9dbcf32713c630ccc23808d86ea70f17ec3e4b12d3722c1f21be1033a04eb752

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	48
Hash anterior (prev_hash)	d7b18f03fb706b50d5990718be2cd7d76abf7892376da94224bc286b4e248703
Hash del registro (record_hash)	b0c44eb2a583db8db4a6eb75f8ac958a3152fdffb0b7dc48454078e5b9a38e9d

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.