



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	ec15fb41-eb3b-4aa0-8bf1-a1857e71fd1b
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 016
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

26 · Vaca

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	b85e51f6f125942f3a1a4131602f3150dbafebdcf07daeb2a9dd46132aade11f
Semilla del cliente (client seed)	sencamer-demo-animalitos-016
Nonce	16
Semilla del servidor (revelada)	ab16b0e8d6c718c27c8fad47d4112cd8f0b23b579f762ceb4a1d7d402aa2877a

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	47
Hash anterior (prev_hash)	bee795914b5e9968cfaf7fe17efc9bc1923e0ee75429264c9d4806a47bc03b7e
Hash del registro (record_hash)	d7b18f03fb706b50d5990718be2cd7d76abf7892376da94224bc286b4e248703

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.