



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	63b8cd73-21e2-471e-87d1-70929ef84f57
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 015
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:08Z
Ejecutado	2026-08-25T05:38:08Z
Revelado	2026-08-25T05:38:08Z

2. Resultado Oficial

46 · Puma

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	b6ac3cae0e79cc7284ee821d6dee92a592767bdbbe93a3e0c45acdb1b9c5b652
Semilla del cliente (client seed)	sencamer-demo-animalitos-015
Nonce	15
Semilla del servidor (revelada)	14f136014fc3f1e8f0cbb13959ed982a02a35331014b631de1378d7424daf105

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	46
Hash anterior (prev_hash)	38d9209862fcbc63e20a952df423e34a354ad29402d9689b9a802004d23759db
Hash del registro (record_hash)	bee795914b5e9968cfaf7fe17efc9bc1923e0ee75429264c9d4806a47bc03b7e

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 $\text{SHA-256}(\text{prev_hash} + \text{datos canónicos})$. El portal público de verificación realiza estos pasos automáticamente.