



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	f98905ef-f6a0-482b-a971-f7bbe8ec1c44
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 004
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:03Z
Ejecutado	2026-08-25T05:38:03Z
Revelado	2026-08-25T05:38:03Z

2. Resultado Oficial

27 · Perro

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	9c9331877547de47aee8d616f9d808674430cf8cbc07e1af90af4bfe44859c0a
Semilla del cliente (client seed)	sencamer-demo-animalitos-004
Nonce	4
Semilla del servidor (revelada)	b8c3bbe291a755a3b8df1d682781c90eeaf0dbad355dac4e718e15d247385069

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	35
Hash anterior (prev_hash)	2923042a0bbda4052043b07eb6e8e3702f993401732ad9950e43a12fdad4ecb0
Hash del registro (record_hash)	15f1e539fc8e5c6740aec93d1b719450a225443c6d1d2341c8e5992ec3eacf4

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.