



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	8c19149e-0590-44e6-b2ab-2e9eedff4f7a
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 013
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:07Z
Ejecutado	2026-08-25T05:38:07Z
Revelado	2026-08-25T05:38:07Z

2. Resultado Oficial

15 · Zorro

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	036c5b9f86a36f03a771d4ae02ce4a67ddb1cf8c3fb0609409e15e4d0ca6bf39
Semilla del cliente (client seed)	sencamer-demo-animalitos-013
Nonce	13
Semilla del servidor (revelada)	0fcdd27d2530bcf7abe86f537b180283dacfb2bd3309b4a7d07935743117ab2

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	44
Hash anterior (prev_hash)	f8e7d82248debe3617fc73d9bd434f3673c400a847e98781b3049031c28465d7
Hash del registro (record_hash)	27ef2041a07a6d0cd91a34b3fd156d53cd075c78459dcab8dac86753d9e378a1

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.