



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	12427929-1326-48d6-bb17-a43781be5308
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 009
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:05Z
Ejecutado	2026-08-25T05:38:05Z
Revelado	2026-08-25T05:38:05Z

2. Resultado Oficial

54 · Grillo

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	d7f5e8cffffd8aad518752ce1c4e8f7ca7949403fa1acf493c47da995d8aa6e8e
Semilla del cliente (client seed)	sencamer-demo-animalitos-009
Nonce	9
Semilla del servidor (revelada)	20b9017e4b515a1330b16c6df323bc8954c1e777f7513dcb686f1d9d24ac21a1

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	40
Hash anterior (prev_hash)	92c48537c68dd5b9183e0829b05476c0bb8a63511db6de95705cbc3319e0e535
Hash del registro (record_hash)	a9a92396cbbdcae8b9da2338b1211d5b57ff08c7293e619b91b2662612995a63

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.