

ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	0b75dec6-64ec-409e-8c4d-8a8843ce669b
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 023
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:12Z
Ejecutado	2026-08-25T05:38:12Z
Revelado	2026-08-25T05:38:12Z

2. Resultado Oficial

29 · Elefante

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	e5d5c66e8a53b66d007788a63f79bc3b72cf37aa533725a980b781498fe06b66
Semilla del cliente (client seed)	sencamer-demo-animalitos-023
Nonce	23
Semilla del servidor (revelada)	3f831a712d671c23ebd7909949a0d832e7e20d163edbfda54d6a4e05abbdfbd6

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	54
Hash anterior (prev_hash)	7b62e32d4bd70589bb261287b77f2c97d7f896ce695cd71a19d85b353ffb94fb
Hash del registro (record_hash)	7fb90c966766cbe22eb944e89f07c8472f4798b2a37b68d9d8d1f83a853114e5

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.