



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	25244c28-9558-4163-af6b-f7dca12a593a
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 021
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:11Z
Ejecutado	2026-08-25T05:38:11Z
Revelado	2026-08-25T05:38:11Z

2. Resultado Oficial

41 · Canguro

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	8859321b11e5b83ce825676a4cccd70df1dc70bf7b72ee282f05bd6eee10f31f
Semilla del cliente (client seed)	sencamer-demo-animalitos-021
Nonce	21
Semilla del servidor (revelada)	9ebb896337fa31825eb6c665aadbb244cea6bc6e3785b50f5e59477dec8e98c1

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	52
Hash anterior (prev_hash)	78d229d851b7018f8c530fd081873b6653991638e1d4aed38866ed386cbd9cf5
Hash del registro (record_hash)	7ed416d47142144a74bd105242627b060326b61715fa7ffc71f6250029bf11da

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.