

ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	ddcd1d84-e7a5-432c-a465-ccb9041003fe
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 020
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

02 · Toro

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	7f19a25864aa82adb23625d687220aff7f6adc99be34fdb8fe528f78ce3d97b
Semilla del cliente (client seed)	sencamer-demo-animalitos-020
Nonce	20
Semilla del servidor (revelada)	37540921a68b6e6e7c5a8b9843497c03f9f91adf0082b3c505555f9bfc9fddd6

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	51
Hash anterior (prev_hash)	77bba057d3fdbef623669367cfea454147acb10fef1b9661dee23e880148ca4c
Hash del registro (record_hash)	78d229d851b7018f8c530fd081873b6653991638e1d4aed38866ed386cbd9cf5

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.