



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	0b3fbed5-9c36-402b-9f50-0cb94e40a5e9
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 019
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:10Z
Ejecutado	2026-08-25T05:38:10Z
Revelado	2026-08-25T05:38:10Z

2. Resultado Oficial

06 · Rana

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	25cca379e06e31b5748e14cbf5d7f0f623ea49f5ca4541d8406152bf64291750
Semilla del cliente (client seed)	sencamer-demo-animalitos-019
Nonce	19
Semilla del servidor (revelada)	c650e5e95f9d7ecca580c62f6d7957deee7cfc5cb47730ca4a9239a3660b1668

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	50
Hash anterior (prev_hash)	d15a9c4d03591496f4b517d87da57aff8d340bf145bb098d0d4a3a5b73b07480
Hash del registro (record_hash)	77bba057d3fdbef623669367cfea454147acb10fef1b9661dee23e880148ca4c

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.