



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	882f5433-a4a6-4f7b-894a-436e1c4889ba
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 014
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:08Z
Ejecutado	2026-08-25T05:38:08Z
Revelado	2026-08-25T05:38:08Z

2. Resultado Oficial

21 · Gallo

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	a5cfa12d4daac88cf605d5dfd51bddc465739366747eceddbd2266bf73fd266
Semilla del cliente (client seed)	sencamer-demo-animalitos-014
Nonce	14
Semilla del servidor (revelada)	c0c49104a3dc2a7be02203aca9e86f3f8dac3b7272b6620dd0d5530430016404

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	45
Hash anterior (prev_hash)	27ef2041a07a6d0cd91a34b3fd156d53cd075c78459dcab8dac86753d9e378a1
Hash del registro (record_hash)	38d9209862fcbc63e20a952df423e34a354ad29402d9689b9a802004d23759db

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.