



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	8f94b7d1-a093-40a8-a7f1-3dba870af5dc
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 001
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:02Z
Ejecutado	2026-08-25T05:38:02Z
Revelado	2026-08-25T05:38:02Z

2. Resultado Oficial

32 · Ardilla

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	3273870656aa111cc4edac8bbb0ec04ebe953511f3f5404f578c864b8f3de935
Semilla del cliente (client seed)	sencamer-demo-animalitos-001
Nonce	1
Semilla del servidor (revelada)	64862aa33a90b3994629751d77e73752509f93df4fcf2e3f33c7d5587f9772a9

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	32
Hash anterior (prev_hash)	e08e2cec99a5b657dbee0e07b51ce0a105b553e83971379f5fec7ce032f4fcf7
Hash del registro (record_hash)	815d6ed5c0335b35b12e1e62049a9e8c0610b0a429a2d57d991d587dd54f7638

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.