



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	9cfbb359-ea9b-4f8a-a647-5c468050d94e
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 007
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:05Z
Ejecutado	2026-08-25T05:38:05Z
Revelado	2026-08-25T05:38:05Z

2. Resultado Oficial

49 · Pereza

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	f577db08fe62e7f8040c125ac9938d767e08f27facb2b6424090d3751b34250d
Semilla del cliente (client seed)	sencamer-demo-animalitos-007
Nonce	7
Semilla del servidor (revelada)	86c19669a17602506761260aa673702347078ffe12d4a8d5ac6de81d67346122

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	38
Hash anterior (prev_hash)	1d7c16e7591b1c6a78dd716634c5cbc898ffe5e7816dde311c3c7a4d84aa7aad
Hash del registro (record_hash)	a31e430cc49db468516c5034ec7979bd9e6a8faf13915d4ef47197de6efbd573

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.