



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	4bf2b409-a884-4a75-b5cf-1dc69adbbafa
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 003
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:03Z
Ejecutado	2026-08-25T05:38:03Z
Revelado	2026-08-25T05:38:03Z

2. Resultado Oficial

30 · Caimán

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	bd6dd327c62e38053c5a11c025da8f2c956ca5f862640728c9bfad55e6d80471
Semilla del cliente (client seed)	sencamer-demo-animalitos-003
Nonce	3
Semilla del servidor (revelada)	36df98ed4e521ef9af9034a99cdd947ae2fb6626ae6a078112f6ac343517463a

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	34
Hash anterior (prev_hash)	f640eb9c288fd7237716b161a288c0d1b44ef7bfdd13613f1adf1cf670f891d4
Hash del registro (record_hash)	2923042a0bbda4052043b07eb6e8e3702f993401732ad9950e43a12fdad4ecb0

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.