

ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	9ca3fc31-6a8b-49a7-a68b-439117607f17
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 018
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

34 · Venado

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	03e4d11648058af30b8671244a91f436db8a980a9ab33eea2d50cc82f0c7d3fa
Semilla del cliente (client seed)	sencamer-demo-animalitos-018
Nonce	18
Semilla del servidor (revelada)	3cbfe56660a98236f2581cf94916d1b30451a8345917ce6fe708da800cda8c75

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	49
Hash anterior (prev_hash)	b0c44eb2a583db8db4a6eb75f8ac958a3152fdffb0b7dc48454078e5b9a38e9d
Hash del registro (record_hash)	d15a9c4d03591496f4b517d87da57aff8d340bf145bb098d0d4a3a5b73b07480

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.