



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	ec5395b0-1509-46a1-9d30-7019559a2566
Nombre	[DEMO SENCAMER] Triple Falcón – Sorteo Digital — muestra 020
Tipo de juego	Triple Falcón
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:37:59Z
Ejecutado	2026-08-25T05:37:59Z
Revelado	2026-08-25T05:37:59Z

2. Resultado Oficial

Triple A: 274 (Terminal 74) · Triple B: 546 (Terminal 46) · Estado: Bolívar

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	0dac793931b7d7cd4916ca01569f4bb1c3c594a30fab65e5f983952bca80fe9
Semilla del cliente (client seed)	sencamer-demo-triple-020
Nonce	20
Semilla del servidor (revelada)	534cefc9627c93fe4ab68c7233df3618f5a42b88e7386a3e21e5f1bd1040712e

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	26
Hash anterior (prev_hash)	9ec30c8076f71c086f631c2957265b16783ddda316cec6129ff9978011524692
Hash del registro (record_hash)	02b0b4f0669e17426241b4772142544f9c335c6e4aeee00843538c967db694ed

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.