



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	907585cb-46be-49b2-a4c4-9293ed5206b5
Nombre	[DEMO SENCAMER] Triple Falcón – Sorteo Digital — muestra 022
Tipo de juego	Triple Falcón
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:00Z
Ejecutado	2026-08-25T05:38:00Z
Revelado	2026-08-25T05:38:00Z

2. Resultado Oficial

Triple A: 235 (Terminal 35) · Triple B: 106 (Terminal 06) · Estado: Táchira

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	f732a1ec38d00c89b8a19b7682e1ebbb72ab00e7c2a01df4ae7f8b3987c0e440
Semilla del cliente (client seed)	sencamer-demo-triple-022
Nonce	22
Semilla del servidor (revelada)	611e33bd349b33d9092c899b165ce874fd81fca187d504bded809781d773ba69

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	28
Hash anterior (prev_hash)	e9453afffa216a4dd30bc1ad6b8cb2bd218799e7cd24af81beee8cc57d86a086
Hash del registro (record_hash)	2d7d8a9f42113fafb631792cb518b8511fd7a080f7110ea8f3719b4a5145156a

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.