SORTIVEN
Sorteador Integral

ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	b79fc206-6907-427b-858d-66f33db2b1fa
Nombre	TEST_mensajes
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T18:37:18.655202+00:00
Ejecutado	2026-10-22T18:37:20.567924+00:00
Revelado	2026-10-22T18:37:22.368008+00:00

2. Resultado Oficial

Triple A: 764 (Terminal 64) · Triple B: 283 (Terminal 83) · Estado: Carabobo

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`847b3ec5f569e9f1e46bca63cfb4e3c45bd3f72cc78b3b026c7e4a1bbdc82097`
Semilla del cliente (client seed)	`46589e3e3a305ce8`
Nonce	1
Semilla del servidor (revelada)	`bdbdf05e5de9e3c76e32f9f4c08b1e1c203095cc6fa106b8fd4570e27b818a4d`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	74
Hash anterior (prev_hash)	`f219895daa2b47b41865e8b589c34b5bbd66c33023f31970a038ecf01d8374e4`
Hash del registro (record_hash)	`fe9b115d6a95df521b1a6b564be6954c4e709531c74f5985fec79ad333eff88f`

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.