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	bde847cf-8352-4013-ab75-4653284488f2
Nombre	TripleFalcón Venezuela — 22/10/2026 18:37
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T18:37:29.346488+00:00
Ejecutado	2026-10-22T18:37:30.513897+00:00
Revelado	2026-10-22T18:37:31.534857+00:00

2. Resultado Oficial

Triple A: 739 (Terminal 39) · Triple B: 787 (Terminal 87) · Estado: Sucre

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`0b4be37b23845db8a2a6808146986ce91794f60de2dac84d4e10f28cc6f5524d`
Semilla del cliente (client seed)	`c2ef42b2fd34fd73`
Nonce	1
Semilla del servidor (revelada)	`7fd8f30a124150cded2efffe3eefccf49ccba801c8dbc53970a01e85b610f47d`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	75
Hash anterior (prev_hash)	`fe9b115d6a95df521b1a6b564be6954c4e709531c74f5985fec79ad333eff88f`
Hash del registro (record_hash)	`3f336ed2321dd35069a1f4171a0ed75e358d5141797985589f4baeec491c7646`

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.