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	efd8f20a-b65a-4ec8-b978-788839f288dd
Nombre	TEST_mensajes
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T18:41:01.276713+00:00
Ejecutado	2026-10-22T18:41:03.154654+00:00
Revelado	2026-10-22T18:41:04.957718+00:00

2. Resultado Oficial

Triple A: 168 (Terminal 68) · Triple B: 745 (Terminal 45) · Estado: Miranda

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`bd1ee569b44a3491f217c41a282664004cdff081c70196b24c55f8d44546e66f`
Semilla del cliente (client seed)	`5eeae178b9216fa0`
Nonce	1
Semilla del servidor (revelada)	`b46ab49ebe142f1b9a7f0ccac19ec24ef074463dafa1e04d03391d7ac7148a86`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	77
Hash anterior (prev_hash)	`4bbc698c72f9fb38d044e8ca436cb1b5ec629ff4b0d245de4b56479b4af09efc`
Hash del registro (record_hash)	`4147803be658d2d3e9558c33f33a09535f618db65c525153938a862a4d15050a`

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.