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	5c25d391-5bff-44c6-a90a-b873b736f74d
Nombre	TEST_mensajes
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T16:53:40.096350+00:00
Ejecutado	2026-10-22T16:53:42.014963+00:00
Revelado	2026-10-22T16:53:43.773851+00:00

2. Resultado Oficial

Triple A: 165 (Terminal 65) · Triple B: 371 (Terminal 71) · Estado: Mérida

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`d888a3fbeaee0cc1b29dcfea00788a80269b4e279573c9084638912fdb354a7b`
Semilla del cliente (client seed)	`cb4a0a80fcdd8aef`
Nonce	1
Semilla del servidor (revelada)	`5c846d285b9bca22185647f3cddc4036950dd882f1741974bc6b6dd1e831600e`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	61
Hash anterior (prev_hash)	`f5cffe747f1fbaf9da25f99cb00c559d9ebce10ad28888b719e9724b17e1a7ef`
Hash del registro (record_hash)	`dad03c65b404403dcf4de068b0243b3d4a51f3a2677768715d942395b34b7125`

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.