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	c5a5c17e-273f-475e-9557-b838e5520bcb
Nombre	TripleFalcón Venezuela — 22/10/2026 18:47
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T18:47:03.655312+00:00
Ejecutado	2026-10-22T18:47:04.517897+00:00
Revelado	2026-10-22T18:47:05.311917+00:00

2. Resultado Oficial

Triple A: 282 (Terminal 82) · Triple B: 913 (Terminal 13) · Estado: Zulia

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`05d560d29361e5c1102f3818e709d651a400fc6c19ce01317b0f00bbf01a1d9a`
Semilla del cliente (client seed)	`3ea57fff723fbcf8`
Nonce	1
Semilla del servidor (revelada)	`585b9eafbddf3a0bbc25ba49588083be791cbd822217299150e09832a0502b9f`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	84
Hash anterior (prev_hash)	`4f0b5e3b536e00981d2af893bc33b7f33ceee664554777cc331fe66c703e91db`
Hash del registro (record_hash)	`d90e961b8a706af07e5ba2729060fb209f832acdb811b748bfd56fac2d1bcc0d`

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.