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	3f726c9c-4cf0-4181-8863-04869abf85f7
Nombre	TripleFalcón Venezuela — 22/10/2026 16:52
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T16:52:02.405663+00:00
Ejecutado	2026-10-22T16:52:03.729054+00:00
Revelado	2026-10-22T16:52:04.785720+00:00

2. Resultado Oficial

Triple A: 703 (Terminal 03) · Triple B: 843 (Terminal 43) · Estado: Amazonas

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`f40ff8b23b7e5db5726fb5f564fbd9ff915e918f4ab19e9729cf7d88bf439a45`
Semilla del cliente (client seed)	`3a619845fd404603`
Nonce	1
Semilla del servidor (revelada)	`e88d46baf10fdcb1f4af6a5b7276cac7af110e58187074bcdba73f4b480cbd1a`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	60
Hash anterior (prev_hash)	`9d7d8982a31964f77b1493f692a06164e03e125bcbc22f9d33f8626431fedad7`
Hash del registro (record_hash)	`f5cffe747f1fbaf9da25f99cb00c559d9ebce10ad28888b719e9724b17e1a7ef`

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.