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	50a61389-078b-4ada-b830-d91fa1128e9a
Nombre	TEST_mensajes
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-11-10T13:10:57.971012+00:00
Ejecutado	2026-11-10T13:10:59.695737+00:00
Revelado	2026-11-10T13:11:01.249070+00:00

2. Resultado Oficial

Triple A: 116 (Terminal 16) · Triple B: 189 (Terminal 89) · Estado: La Guaira

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`65d86cc53fb0f23cbc76aba32096795534aa086fa9c50bda15c33a418baefb2e`
Semilla del cliente (client seed)	`8b673e0d6a658c3f`
Nonce	1
Semilla del servidor (revelada)	`8fcd188a3b96f6289dfe55196e95d91bbcef51ca9e818f45b2a4c0bf6cba11b9`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	132
Hash anterior (prev_hash)	`e9c3b1a4a4632d50ca00432d126a182cd7da274e43ada3961db7ee6065cfe4e6`
Hash del registro (record_hash)	`03fa11f27390e75756b2302234d54e133e1863dfb406cd7838677c65b32299f2`

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.