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	b85eaa66-9dfb-439c-acd8-066fbdcb8d41
Nombre	TEST_mensajes
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T16:57:41.028461+00:00
Ejecutado	2026-10-22T16:57:42.967933+00:00
Revelado	2026-10-22T16:57:44.666949+00:00

2. Resultado Oficial

Triple A: 751 (Terminal 51) · Triple B: 564 (Terminal 64) · Estado: Portuguesa

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`165e72bcc48aae64a7e721d4e13c6ed76ae06b5e76fcb3504e91decb3d3a5194`
Semilla del cliente (client seed)	`285980cebad846ab`
Nonce	1
Semilla del servidor (revelada)	`b1ec045d197e3bf8b6149dcb26b74439133760d659eb40f1e91385931f626ef0`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	68
Hash anterior (prev_hash)	`a70898d7239093016e1156d9d394d02c196654a892f423ca752a638319bd5802`
Hash del registro (record_hash)	`7fe3bdb97d04b82039c7c5f5b2dc82e082be7d1c14345ecbab75fee0c9e2de65`

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.