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	5eb56cc6-2adf-4345-a41a-edce134280e4
Nombre	TEST_mensajes
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T16:57:01.627299+00:00
Ejecutado	2026-10-22T16:57:03.392335+00:00
Revelado	2026-10-22T16:57:05.006553+00:00

2. Resultado Oficial

Triple A: 803 (Terminal 03) · Triple B: 769 (Terminal 69) · Estado: Portuguesa

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`d432865f1d801718464ed44023fbd475b53d0e12ce33cff0c91c8778c9225309`
Semilla del cliente (client seed)	`650ad86689540194`
Nonce	1
Semilla del servidor (revelada)	`e966ebabd0ce72ac2ffd56be82311751f9e11b12b6a5f0e687af9433ad406547`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	66
Hash anterior (prev_hash)	`42931ea6ca352cddc590321e167c5829f29c92e80ec779a60d298cdeb1bde9b8`
Hash del registro (record_hash)	`50a096ca41869917e22611f4f502ba4569535922aa295aa3696c337f2466cbb1`

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.