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	c449267b-f1b8-48a1-ae5f-8796bcf78abe
Nombre	TripleFalcón Venezuela — 22/10/2026 16:57
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T16:57:12.456959+00:00
Ejecutado	2026-10-22T16:57:13.793798+00:00
Revelado	2026-10-22T16:57:14.856758+00:00

2. Resultado Oficial

Triple A: 494 (Terminal 94) · Triple B: 684 (Terminal 84) · Estado: Falcón

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`66433528f7d1ae64fc7e0ad7be4f26420fe216319e9eaa176228215ae60e857c`
Semilla del cliente (client seed)	`f67c60fba7c1ef18`
Nonce	1
Semilla del servidor (revelada)	`b59cc72d1bd859a6c88e58e3d1bfcd7c9889275f45881b092155a42b2eb70294`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	67
Hash anterior (prev_hash)	`50a096ca41869917e22611f4f502ba4569535922aa295aa3696c337f2466cbb1`
Hash del registro (record_hash)	`a70898d7239093016e1156d9d394d02c196654a892f423ca752a638319bd5802`

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.