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	91535df5-d80a-495f-8156-486d76a6e474
Nombre	TripleFalcón Venezuela — 22/10/2026 16:56
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-22T16:56:37.238929+00:00
Ejecutado	2026-10-22T16:56:38.621790+00:00
Revelado	2026-10-22T16:56:39.719823+00:00

2. Resultado Oficial

Triple A: 160 (Terminal 60) · Triple B: 475 (Terminal 75) · Estado: Trujillo

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`e00b83139112d6d6447caa44e712932aa754270ad9ebe0920feb690d7b6e9c6c`
Semilla del cliente (client seed)	`9b491179d4302e6c`
Nonce	1
Semilla del servidor (revelada)	`6d6edc266d35b2f48d12afecf40f7957ff53a3e71280294c70916128368329cd`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	65
Hash anterior (prev_hash)	`88c205f48c38894dacda79a79c3c9f67d564c2f4ca664c025021073cdf8c8a83`
Hash del registro (record_hash)	`42931ea6ca352cddc590321e167c5829f29c92e80ec779a60d298cdeb1bde9b8`

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.