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	557e76ab-f2e2-487e-a23f-6103cdd79573
Nombre	TripleFalcón Venezuela — 20/10/2026 17:31
Tipo de juego	TripleFalcón Venezuela
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-10-20T17:31:38.098640+00:00
Ejecutado	2026-10-20T17:31:39.527924+00:00
Revelado	2026-10-20T17:31:40.665930+00:00

2. Resultado Oficial

Triple A: 616 (Terminal 16) · Triple B: 682 (Terminal 82) · Estado: Distrito Capital

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`072ab5ca5a3b5d3bc823fc670be8b2a647ed3089717e7ac84be95e05166a5736`
Semilla del cliente (client seed)	`cb27e26fc3f43cc9`
Nonce	1
Semilla del servidor (revelada)	`f625a498efa3af003a7ef27a98f3394b18c43a1d504908899212c17e62e0f38d`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	57
Hash anterior (prev_hash)	`2d5dd75e6b425e3d521546ddf05fae28995b2e904f9c899e83fe5030ccb7a76f`
Hash del registro (record_hash)	`201d733f78d649a32eb3ea5b7507f8f92d44ccc295a2838d33a34e9539c5bc7e`

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.