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	972784ed-4b06-4626-9938-8a5ae5104d4d
Nombre	Loto Zumba — 10/11/2026 12:37
Tipo de juego	Loto Zumba
Ente supervisor	Junta de Beneficencia Pública y Asistencia Social del Estado Bolivariano de Mérida (Lotería de Mérida)
Operadora	Operadora Zumba, C.A.
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-11-10T12:37:39.608954+00:00
Ejecutado	2026-11-10T12:37:40.526248+00:00
Revelado	2026-11-10T12:37:41.366673+00:00

2. Resultado Oficial

23 · CEBRA

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`12b26292fe676a3040688d40f97e408fce8a9e02bff27a34be1cee2115464e40`
Semilla del cliente (client seed)	`27363ac482fc47d7`
Nonce	1
Semilla del servidor (revelada)	`c3832050fbe9c0efe61423fd674dedc9e46ac47cd01d41484e240f11424c1604`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	112
Hash anterior (prev_hash)	`abaac9a8d7ed36429f208f44d6ec9e7cf9444dc96752aebcc1b07b31a66d5044`
Hash del registro (record_hash)	`e9117e4b7d699a06afa797f9b61269bd159f6a8222d3dd4e745141115a51bcb1`

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.

Documento generado automáticamente el 2026-11-23 10:49:53 UTC. Este acta es un artefacto de auditoría reproducible.