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	02d5e3d3-b503-4d95-8c2c-a5fa75a09de4
Nombre	Loto Zumba — 10/11/2026 12:33
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	2026-11-10T12:33:43.662906+00:00
Ejecutado	2026-11-10T12:33:44.840183+00:00
Revelado	2026-11-10T12:33:45.674634+00:00

2. Resultado Oficial

13 · MONO

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`ab9917a4fb29968fdf1ca26998360919b29e53de6c59581bf282cb46f1b37fe8`
Semilla del cliente (client seed)	`fec34c22b5501046`
Nonce	1
Semilla del servidor (revelada)	`615f6197c3e6d391e4cebcc3d21cfc354f4e699c579fa19cb6cb8be360d02082`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	101
Hash anterior (prev_hash)	`d41cc8765ad4767bc2ca71f5fb448153a3a7336a76d7303e37870fc7a479a270`
Hash del registro (record_hash)	`9eecc6c4bd12e4fef58282527c25bf6f97eda5d37ea38ff8854d10ebd444a7e9`

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 10:57:25 UTC. Este acta es un artefacto de auditoría reproducible.