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	ba252638-0749-4e20-a98d-1a95b3cc7530
Nombre	Loto Zumba — 10/11/2026 13:06
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	2026-11-10T13:06:17.994513+00:00
Ejecutado	2026-11-10T13:06:19.142401+00:00
Revelado	2026-11-10T13:06:20.067904+00:00

2. Resultado Oficial

03 · CIEMPIÉS

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`d2f0f35c04e9ab1278ffcc111ff799af8f214d6e42f8aa9457e45b1e8f4780dc`
Semilla del cliente (client seed)	`835412f2c305c7df`
Nonce	1
Semilla del servidor (revelada)	`f0a3cb893892fa173ab602d2d369a4dc026f4199d9a8691747a16876b5bd3700`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	125
Hash anterior (prev_hash)	`041def0d3ba694f548f0a51dfcebc1fead17f391ef302d6ebd9db519476c0788`
Hash del registro (record_hash)	`622c70d18370fbce868f00a0a3abc59d6d0a3dc331b2833d813485dd2e6b313e`

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 10:59:10 UTC. Este acta es un artefacto de auditoría reproducible.