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	94277242-5814-48a6-a0a5-037b9bf89447
Nombre	Loto Zumba — 10/11/2026 13:04
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	2026-11-10T13:04:14.922181+00:00
Ejecutado	2026-11-10T13:04:16.020210+00:00
Revelado	2026-11-10T13:04:16.931398+00:00

2. Resultado Oficial

30 · CAIMAN

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`561d62e7c3813d1bd7002ce4fbf460da45a6f19ead43a249bf8d4551d210a7ba`
Semilla del cliente (client seed)	`e6838daa8e1b5048`
Nonce	1
Semilla del servidor (revelada)	`46a5c3ea91b23a0d9326748d3ee6f227f53a285b7c26124cb82b6d0f4c4f9097`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	114
Hash anterior (prev_hash)	`789ea841918183e1b3946f521a067be06587f835e689bad3154018001cd3931d`
Hash del registro (record_hash)	`8b5028842a5134c24f6ea5aa8a011bb5a50df5bc6f4c8297dbb177500b874db0`

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 10:57:22 UTC. Este acta es un artefacto de auditoría reproducible.