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** | 8594d8d4-5437-43b9-b627-e418e9f12cbd |
| **Nombre** | Loto Zumba — 10/11/2026 12:36 |
| **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** | 2026-11-10T12:36:51.350629+00:00 |
| **Ejecutado** | 2026-11-10T12:36:52.334292+00:00 |
| **Revelado** | 2026-11-10T12:36:53.242196+00:00 |

## 2. Resultado Oficial

## 69 · CONEJO

## 3. Evidencia Provably-Fair

| | |
|---|---|
| **Compromiso (SHA-256) — pre-sorteo** | `ff000e2a00b401fe143b93ac87065276bd2289940c7da1d28a00259e0fea162f` |
| **Semilla del cliente (client seed)** | `2477224a2e33be08` |
| **Nonce** | 1 |
| **Semilla del servidor (revelada)** | `da0dcd9d5a2c050bc0c15787d4d10ccac321414916344e721eee60ecf9222a7a` |

## 4. Cadena de Auditoría (Ledger inmutable)

| | |
|---|---|
| **Índice en la cadena** | 106 |
| **Hash anterior (prev_hash)** | `07a1897a762f95c239f7c96a3af5622cf84be58dd391714bee0bbc89da3f227d` |
| **Hash del registro (record_hash)** | `8976486208776da9c482912017988a7f59fabcb65e0e2b5be0593908c30b725f` |

## 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 10:49:40 UTC. Este acta es un artefacto de auditoría reproducible.