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	b06b3c06-2f03-480c-8d73-be889f87417b
Nombre	Loto Zumba — 10/11/2026 12:30
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	2026-11-10T12:30:27.328779+00:00
Ejecutado	2026-11-10T12:30:28.442310+00:00
Revelado	2026-11-10T12:30:29.327991+00:00

2. Resultado Oficial

28 · ZAMURO

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`eef5d526e0f21ce80fd33ab3e99c1d8af5cc90a937ed4df8a4e99a0ddcb1f003`
Semilla del cliente (client seed)	`d7ba88b6e9157c67`
Nonce	1
Semilla del servidor (revelada)	`59c72d490187e702ad37f2ad848be06aa93819d6f46f93516ca239e3259ee782`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	90
Hash anterior (prev_hash)	`34ed74c93285790d4b6254a55e650fcf648afd569acf872c910ea63118c1446e`
Hash del registro (record_hash)	`633fbbfc3d3158d7883c992078a9ca8e672c96b8d9a87a1f4900b10a23603cba`

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 10:59:15 UTC. Este acta es un artefacto de auditoría reproducible.