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	bdbd6ddf-5ded-498d-8717-b0b182419cf1
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	2026-11-10T12:30:51.081006+00:00
Ejecutado	2026-11-10T12:30:52.231753+00:00
Revelado	2026-11-10T12:30:53.162620+00:00

2. Resultado Oficial

38 · BÚFALO

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`e0437a03a9fe29f476f32c7f07abbd9a58b37be70421bf91126e6d2fe1af5c8b`
Semilla del cliente (client seed)	`70dea3ef5e3b882c`
Nonce	1
Semilla del servidor (revelada)	`745ce683e0b2abdbf82b5c657f6127a37b3112145f7db77fc7f0fbdcf183ec3e`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	91
Hash anterior (prev_hash)	`633fbbfc3d3158d7883c992078a9ca8e672c96b8d9a87a1f4900b10a23603cba`
Hash del registro (record_hash)	`079debabd8c70b903351a5cfbf742f12fd4ab0406cc9f08fd9758a4d8162400b`

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 10:59:22 UTC. Este acta es un artefacto de auditoría reproducible.