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	46ef3d38-0449-47da-9440-c7ad77cca078
Nombre	Loto Zumba — 10/11/2026 13:05
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	2026-11-10T13:05:34.689145+00:00
Ejecutado	2026-11-10T13:05:35.671110+00:00
Revelado	2026-11-10T13:05:36.924822+00:00

2. Resultado Oficial

69 · CONEJO

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`ad0df9a57f9000cb37a186fa8095185358d7c3f39e832cc628e0f1862dc83326`
Semilla del cliente (client seed)	`4bdfad2aa4c043c6`
Nonce	1
Semilla del servidor (revelada)	`1e36fb59dcbf300699fddaad6c3041805a6ddfab01c416877068b9bff3379bd9`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	120
Hash anterior (prev_hash)	`b2383f4fafe80c444e086f6111df1f3b8b838e62974d0a1b7152b72ccc236f68`
Hash del registro (record_hash)	`3d091396645c4423ac078d5ab08e42f8d446fcb560393061455d065a967f9cf3`

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 10:59:28 UTC. Este acta es un artefacto de auditoría reproducible.