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	22632d40-e620-48d0-89e1-61d8b3c23d61
Nombre	TEST_iter8 zumba
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	ejecutado
Versión del algoritmo	rng-v1
Creado	2026-11-10T13:07:08.628308+00:00
Ejecutado	2026-11-10T13:07:16.798079+00:00
Revelado	None

2. Resultado Oficial

55 · OSO HORMIGUERO

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`b23bd066e10635a193de6144212b8315c32d4dffebdcd8bea841f61394f1a33d`
Semilla del cliente (client seed)	`66020a291914ad7b`
Nonce	1
Semilla del servidor (revelada)	`Aún no revelada`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	127
Hash anterior (prev_hash)	`504ecaff77bf5b39621adef562ea2ae5ecd68e5aaf9d437bec48386df3293f36`
Hash del registro (record_hash)	`d8109c5f355e284cce49cae846361b3f35488337da4744c22a8a8e5dfb655a97`

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 10:50:23 UTC. Este acta es un artefacto de auditoría reproducible.