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	f222c103-dcc6-46ca-9256-d1e1991558e1
Nombre	Loto Zumba — 10/11/2026 13:10
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	2026-11-10T13:10:31.790049+00:00
Ejecutado	2026-11-10T13:10:32.795381+00:00
Revelado	2026-11-10T13:10:33.816616+00:00

2. Resultado Oficial

21 · GALLO

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	`21ff54f7ab093e22b770e86b957aa51be5598bf301099dda60692fa34af55b9d`
Semilla del cliente (client seed)	`f107bc60bd901ce9`
Nonce	1
Semilla del servidor (revelada)	`688f4b7e317351f22d7653d4ac306a22dc58388dc48777d3d50097ca37fca5c3`

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	129
Hash anterior (prev_hash)	`d490ea1b8447e07888e82ee2efcf6b8bed401273ec32cb37275a421e75063047`
Hash del registro (record_hash)	`2fa643e66b38747009398e2a9eb794b3f13625f653b8e59efd5a8856af830d26`

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 10:52:50 UTC. Este acta es un artefacto de auditoría reproducible.