



ACTA DE SORTEO CERTIFICADO

SORTIVEN V1.4 — Sistema de Sorteo Auditable · Aleatoriedad Verificable (Provably Fair)

1. Identificación del Sorteo

ID del sorteo	42a3cc13-31e2-4ee2-b81c-5ecb4d1a27e9
Nombre	sorteo prueba 1 julio
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-07-13T02:17:24.758123+00:00
Ejecutado	2026-07-13T02:17:43.453099+00:00
Revelado	2026-07-13T02:17:48.888130+00:00

2. Resultado Oficial

38 · Búfalo

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	489d61bcb90011a3eee643cd1edb54fde992725d1e6aba7d46fff5653e11b106
Semilla del cliente (client seed)	eb1a807b41f7387c
Nonce	1
Semilla del servidor (revelada)	3632da5deac4f29dbeefb3d77f50cf08ae2272830b8b18f1331890466139a5a7

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	4
Hash anterior (prev_hash)	260fa5dbd3c7507356d16d20c469dd998fef2ff618a2ba15d378dc4e03227740
Hash del registro (record_hash)	6debda5c40ad227ca6dc561309d52941507b071036593010b2882e47a49954f2

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.