



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	f234fee8-866d-4897-826d-5c22d2f4f053
Nombre	prueba 1 a
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-06-03T20:02:06.505298+00:00
Ejecutado	2026-06-03T20:07:44.303038+00:00
Revelado	2026-06-03T20:07:48.588263+00:00

2. Resultado Oficial

51 · Pelicano

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	837ce4d9c7c5ca7a143c20003332d77a6b9d0a704fcb37c59e21a5013b56f5f9
Semilla del cliente (client seed)	d6b8f7b78f84404c
Nonce	1
Semilla del servidor (revelada)	58a4cd4994a7ddf5a8d04dff762b7aa5fc2eddf85153c1ac9dc4eb813293b8c0

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	1
Hash anterior (prev_hash)	7c40c28afae532502ee65ef916c3c08477c5b1add31569ddf5f234e6f231f6c6
Hash del registro (record_hash)	72366232d58aa46f999cea688f186e87d717cef76d1044b3c9dace78c96e405f

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.