



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	ea6bcc68-b996-47cd-9f6c-3c0a83a16c0c
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 022
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:12Z
Ejecutado	2026-08-25T05:38:12Z
Revelado	2026-08-25T05:38:12Z

2. Resultado Oficial

35 · Jirafa

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	ad830b6c3a3cf8fb1af32cc8b593fa49fe3804afdd3919f350747c28f9b8228c
Semilla del cliente (client seed)	sencamer-demo-animalitos-022
Nonce	22
Semilla del servidor (revelada)	8e2169fd34efc03b833c8e24a4c87bff8c72bbff08a97f0e259dee06fcc90f3d

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	53
Hash anterior (prev_hash)	7ed416d47142144a74bd105242627b060326b61715fa7ffc71f6250029bf11da
Hash del registro (record_hash)	7b62e32d4bd70589bb261287b77f2c97d7f896ce695cd71a19d85b353ffb94fb

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.