



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	1fad455-54bb-460c-93f9-209acd5d7568
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 024
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:13Z
Ejecutado	2026-08-25T05:38:13Z
Revelado	2026-08-25T05:38:13Z

2. Resultado Oficial

29 · Elefante

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	ffe0c34e3d47c67c2a7ad93aab5eafe6635fd843226f9fd72084fdefc4d36d2a
Semilla del cliente (client seed)	sencamer-demo-animalitos-024
Nonce	24
Semilla del servidor (revelada)	de05c5eae6800e3a696a83ad94f156ef1482a12a71f7b1fb1026617980bc7e8f

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	55
Hash anterior (prev_hash)	7fb90c966766cbe22eb944e89f07c8472f4798b2a37b68d9d8d1f83a853114e5
Hash del registro (record_hash)	795152170d6334172cff6be2e000efc01fbb3dc10bcb01f467cacb212428bbcc

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.