



ACTA DE SORTEO CERTIFICADO

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

1. Identificación del Sorteo

ID del sorteo	eb5eb574-04fc-4cc7-a7ff-137d3cfd189c
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 025
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

12 · Caballo

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	f76d04acbf75be08e6e92e821c43e4cf06433386900661d4a7332ba52ebe7229
Semilla del cliente (client seed)	sencamer-demo-animalitos-025
Nonce	25
Semilla del servidor (revelada)	ffbc71b4c0ece7f398722c245a1116f3aac6bf207e63db939dbb5526049cb1c3

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	56
Hash anterior (prev_hash)	795152170d6334172cff6be2e000efc01fbb3dc10bcb01f467cacb212428bbcc
Hash del registro (record_hash)	2d5dd75e6b425e3d521546ddf05fae28995b2e904f9c899e83fe5030ccb7a76f

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.