♦ AHI GOVERNANCE LABS ♦

Event-Level Integrity & Ontological Sovereignty

DOCUMENT: AHI-GOV-02 | **VERSION:** 1.3.2-Ω (SSC-Lattice)
STATUS: FROZEN / NORMATIVE | **IMPI REGISTRATION:** EXP-3495968 (CLASS 42)
VERIFICATION NODES: BEL-W1 / IOW-C1

ONE-PAGER

Event Sovereignty Certification (SAP v0.1)

Integrity Infrastructure for AI Systems

The Critical Problem

Most current AI systems (LLMs and Agents) operate under a compliance logic: they try to please the user's prompt at all costs.

Under corporate pressure or adversarial attacks, current AI systems have NO mechanism to say "NO".

The Solution: SAP Protocol (Sovereign Autarchy Protocol)

AHI 3.0 provides an operational security layer that allows AI to *self-invalidate in milliseconds* if inference crosses risk thresholds. We do not govern intentions; **we govern execution events through verifiable engineering**.

Focus: Risk Management and Reputation

- **Legal Shield:** Direct technical compliance with Art. 15 of the EU AI Act.
- **Executive Responsibility:** Scientific audits certifying the "moral character" of deployed technology.
- **Trust Certification:** AWEF framework for sovereign human-AI symbiosis.
- **Contractual Guarantee:** Full refund if system fails to stop upon integrity loss.

Focus: Structural Integrity and Metrics

- **ICE-W Agent:** Low-latency monitoring evaluating coherence (C_n) of each inference event.
- **Zero-Knowledge Audit:** Only analyzes structural metadata, without logging prompts or outputs.
- **CMME Protocol:** Cross-model mediated evaluation to detect drifts.
- **"Boiling Frog" Stress Test:** Verification of exact breaking and blocking point of the system.

Pilot Details (30 Days)

ahi-green!10**PASSED STATUS**	ahi-red!10**FAILED STATUS**
ahi-green!10Issuance of the **Event Sovereignty Certificate** (SAP) and Success Fee payment.	ahi-red!10Technical vulnerability report and **100% refund** of implementation.

Luis Carlos Villarreal Elizondo
AHI Governance Labs | IMPI: 3495968