MANUAL DE BUENAS PRÁCTICAS: PROTOCOLO S.A.A.R.E.

GUÍA DE OPERACIÓN AUTÓNOMA, INTEGRIDAD DE DATOS Y CUMPLIMIENTO NORMATIVO

Este documento establece las directrices obligatorias y recomendaciones operativas para la ejecución del **Protocolo S.A.A.R.E. (Sistema de Alineamiento, Auditoría y Resiliencia Estructural)**. Su objetivo es garantizar el aislamiento de la infraestructura nativa, mitigar la entropía estocástica y asegurar que la desviación lógica se mantenga estrictamente por debajo del umbral crítico preestablecido.

1. Arquitectura de Desacoplamiento Operativo

Para preservar el régimen de Secreto Industrial y evitar brechas de seguridad o intentos de ingeniería inversa, el protocolo debe operar siempre de manera externa e independiente a la infraestructura del cliente.

- **Ejecución Perimetral:** El protocolo jamás debe integrarse en caliente dentro del núcleo del modelo de Inteligencia Artificial (LLM) o base de datos del licenciatario. Debe actuar como una capa de verificación perimetral (*output-side filtering*).
- **Tratamiento de Inputs/Outputs:** Las cadenas de datos e inferencias deben ser interceptadas en formato plano o estructurado (JSON/XML) una vez finalizado el proceso de generación del sistema del cliente, antes de su almacenamiento definitivo o exposición al usuario final.
- **Manual de Ejecución Restringido:** El manual de comandos provisto al licenciatario solo debe contener los parámetros de consulta y las llamadas de ejecución autónoma. Los algoritmos de control de contexto y la lógica determinista subyacente deben permanecer inaccesibles en los nodos de cómputo del licenciante.

2. Monitorización del Umbral de Tolerancia Crítico

El núcleo operativo de S.A.A.R.E. se fundamenta en mantener el diferencial de integridad estructural bajo una restricción matemática estricta:

Protocolo de Actuación según el Nivel de Desviación:

Estado de Desviación	Métrica de Control	Acción Requerida
Zona Verde	$\Delta < 0.01\%$	Integridad óptima. El protocolo valida el flujo de datos de forma automatizada emitiendo el Veredicto de Integridad positivo.
Zona Ámbar	$0.01\% \leq \Delta \leq 0.05\%$	Degradación contextual leve. El protocolo emite una alerta preventiva. Se exige la re-ejecución inmediata del flujo de inferencia.
Zona Roja	$\Delta > 0.05\%$	Quiebre estructural o riesgo de plagio. El protocolo ejecuta un bloqueo forense preventivo inmediato y emite un informe crítico.

3. Ejecución de Auditorías de Propiedad Intelectual (IP)

El módulo de Auditoría de IP está diseñado para blindar a la organización ante reclamaciones de terceros por infracción involuntaria de derechos de autor o patentes.

- **Frecuencia de Muestreo:** En contratos estándar con límites de uso (ej. 3 informes/mes), se recomienda programar las auditorías morfológicas en los hitos de entrega críticos o cierres de versiones de software, optimizando el consumo de consultas del paquete contratado.
- **Contraste de Matriz Lógica:** Al auditar código fuente o plantillas contractuales automatizadas, el operador debe asegurarse de que el protocolo tenga acceso a los repositorios de consulta indexados o, en su defecto, configurar el modo de análisis sintáctico abstracto para detectar similitudes estructurales sospechosas.
- **Custodia del Dictamen:** Todo informe generado por el módulo de IP que arroje un resultado libre de plagio debe ser archivado de forma inmutable. Este documento constituye la prueba legal de diligencia debida ante posibles litigios de marcas o patentes.

4. Gobernanza y Certificación Corporativa (AI Act Compliance)

De acuerdo con las normativas vigentes de gobernanza de Inteligencia Artificial, el protocolo S.A.A.R.E. actúa como un registro forense auditable.

- **Inmutabilidad de Registros:** Los KPIs ejecutivos de cumplimiento y los documentos de Certificación Corporativa generados por el protocolo deben ser almacenados bajo políticas de "Solo Lectura" (WORM - *Write Once, Read Many*) para evitar alteraciones retroactivas.
- **Trazabilidad Forense:** Cada informe debe incluir de manera obligatoria: la marca de tiempo exacta (timestamp), el identificador del nodo de ejecución, el hash del volumen de datos analizado y el valor numérico exacto de Δ obtenido.
- **Presentación ante Inspecciones:** Ante una auditoría regulatoria interna o externa, el licenciatario presentará directamente el consolidado de Certificaciones S.A.A.R.E. como evidencia objetiva de control de riesgos y alineamiento determinista del sistema de IA.

5. Seguridad Jurídica y Confidencialidad del Operador

Las credenciales de acceso temporal para la operación autónoma del protocolo son de uso exclusivo de los técnicos designados por el licenciatario. Queda prohibida su compartición fuera del entorno controlado de evaluación.

Cualquier intento de monitorizar los tiempos de respuesta detallados, forzar desbordamientos de memoria del protocolo o realizar análisis estáticos de los flujos de comando para deducir la topología de los nodos activará la resolución del servicio y la Penalización Resarcitoria de 50.000,00 € estipulada por contrato.