ARQUITECTURA SOLVEOX

Diseño de Gobernanza de IA, Mitigación de Riesgos y Plataforma LegalTech

RESUMEN EJECUTIVO

SOLVEOX es un diseño de arquitectura conceptual para un *marketplace* integral de intermediación de oficios y servicios profesionales remotos. El modelo resuelve la crisis de confianza y seguridad en el mercado informal mediante una infraestructura institucional basada en cinco pilares de gobernanza: validación biométrica de grado Fintech, resolución alternativa de litigios (ADR) in-house, retención transaccional (Escrow), evidencia visual inmutable (Escudo Legal) y cumplimiento tributario automatizado.

El ecosistema está diseñado bajo el principio de *Compliance by Design*, blindando a la plataforma de contingencias por subordinación laboral, reduciendo la exposición civil y anticipando de forma temprana (Readiness) los marcos regulatorios internacionales para evitar fricción operativa y costos de remediación tecnológica.

ESTRATEGIA DE CUMPLIMIENTO NORMATIVO Y ALINEACIÓN EU AI ACT

La arquitectura de SolveoX ha sido diseñada proactivamente anticipando las exigencias dogmáticas de transparencia y control de la regulación europea.

- **Clasificación y Recalibración de Riesgo:** Los algoritmos de derivación logística operan inicialmente bajo un marco de riesgo limitado/mínimo (**Art. 50, EU AI Act**). No obstante, la arquitectura integra una cláusula de Recalibración Dinámica: si el marketplace escala hacia servicios esenciales (ej. mantenimiento de infraestructuras críticas), el sistema cuenta con la trazabilidad

necesaria para transicionar al cumplimiento de Sistemas de Alto Riesgo (**Anexo III, punto 4**).

- **Protocolo Human-in-the-loop (HITL):** En estricto cumplimiento del **Art. 14 del EU AI Act**, la Inteligencia Artificial en el módulo de Análisis de Disputas actúa exclusivamente como soporte de Procesamiento de Lenguaje Natural (NLP). La decisión jurisdiccional, la liberación de fondos Escrow y la categorización de negligencia recaen en un 100% bajo supervisión humana calificada, mitigando el riesgo de automatización sesgada.

- **Transparencia Algorítmica:** El sistema de "Derivación Equitativa" cuenta con métricas explicables (**Art. 13, EU AI Act**), priorizando proximidad y tiempo de respuesta (ETA), neutralizando sesgos de afinidad o penalizaciones invisibles (*Shadowbanning*) que afecten la libre competencia.

GOBERNANZA ALGORÍTMICA Y GESTIÓN DE RIESGOS (NIST AI RMF)

La mitigación de vulnerabilidades técnicas y legales se estructura bajo los cuatro pilares del *NIST Artificial Intelligence Risk Management Framework*:

- **GOVERN (Gobernanza):** Establecimiento de políticas inquebrantables de retención de datos. El material videográfico está sujeto a encriptación asimétrica, mitigando el riesgo de fuga de datos sensibles y limitando el acceso exclusivamente a los oficiales de cumplimiento autorizados.

- **MAP (Mapeo):** Identificación temprana de riesgos de privacidad en integraciones de terceros. Se evalúa el ciclo de vida de los datos biométricos capturados en la fase de Onboarding, asegurando que el proveedor de validación del servicio no almacene la biometría para entrenamiento de modelos fundacionales ajenos.

- **MEASURE (Medición):** En alineación con la norma **ISO/IEC 42001 (Cláusula 9)**, se ejecuta una auditoría continua de la tasa de fricción (disputas) frente a la tasa de éxito (Match) para prevenir desviaciones estocásticas y sesgos demográficos en la asignación de servicios.

- **MANAGE (Gestión):** Implementación de "Bóvedas de Evidencia" y geocercas ofuscadas. Las rutas de tránsito (GPS) de los trabajadores se difuminan para el cliente hasta el momento de llegada (ETA), protegiendo la integridad física y el riesgo de seguimiento malicioso.

LEGAL–TECH Y PROPIEDAD INTELECTUAL

La gobernanza legal sobre las integraciones API externas impone controles estrictos para proteger los activos de la plataforma:

- **Acuerdos de Nivel de Servicio (SLA) y NDAs Estructurales:** Los contratos de desarrollo exigen la transferencia total del código fuente y accesos raíz, incluyendo cláusulas absolutas contra la inserción de *backdoors* o código malicioso.

- **Protección contra Data Scraping:** Los Acuerdos de Procesamiento de Datos (DPA) incluyen adendas que prohíben explícitamente el uso de metadatos o biometría de los usuarios para el re-entrenamiento de LLMs corporativos de terceros.

- **Privacidad por Diseño (Privacy by Design):** Cumplimiento nativo del **Art. 25 del RGPD**. Integración de la directiva técnica FLAG_SECURE en el entorno móvil para anular capturas de pantalla, forzando la seguridad de la información desde la capa de código.

INFRAESTRUCTURA OPERATIVA Y PROTOCOLOS DE SEGURIDAD

- **Validación Biométrica (KYC Estricto):** Escaneo OCR de documento de identidad, *Liveness Check* y validación de antecedentes. Renovación semestral obligatoria bloqueada por sistema hasta la actualización documental.

- **Escudo Legal y Cumplimiento GDPR:** El prestador debe grabar un video continuo in-app del área de trabajo. Para mitigar la fricción normativa respecto a la captura de imágenes en domicilios privados (**Art. 35, RGPD - Evaluación de Impacto**), el sistema proyecta el uso de *Edge Computing* para el procesamiento y difuminación local de rostros de terceros. El material final se encripta en [Infraestructura_Cloud_Tier_1] bajo políticas de retención transitoria.

- **Segregación Financiera (Escrow):** Los fondos del cliente se retienen en una cuenta transaccional separada del capital operativo de la empresa (OPEX), alineándose con los estándares internacionales sobre retención de capitales de terceros e iniciación de pagos.

RESOLUCIÓN DE CONFLICTOS Y ARBITRAJE DE EQUIDAD

- **Autocomposición Asistida (Fase 1):** Obligatoriedad sistémica de intentar un acuerdo directo vinculante en el chat de la plataforma antes de escalar una disputa.

- **Arbitraje Forense Vinculante (Fase 2):** Implementación de un mecanismo de Resolución Alternativa de Litigios (ADR) preferente. Las controversias se someten al Centro de Resolución interno,

fallando con base exclusiva en telemetría inmutable (GPS y video encriptado), bloqueando cláusulas que puedan considerarse abusivas en jurisdicciones europeas.

- **Mitigación de Riesgo Moral:** Los daños accidentales activan automáticamente un "Deducible por Siniestro" que se debita al trabajador (*Skin in the game*). La negligencia inexcusable deriva en expulsión biométrica definitiva del ecosistema.

DINÁMICA CONTRACTUAL Y EXENCIÓN DE SUBORDINACIÓN

- **Autonomía Operativa Absoluta:** La plataforma opera estrictamente como infraestructura tecnológica de intermediación. Se garantiza la libertad tarifaria final y la inexistencia de controles de jornada, blindando el modelo de negocio contra presunciones de laboralidad y reduciendo la exposición a litigios laborales.

- **Cumplimiento Tributario:** Integración API para la emisión automatizada de comprobantes fiscales electrónicos, aplicando las retenciones legales vigentes de forma transparente y garantizando la probidad del flujo de capital.

- Contacto Ejecutivo: *jhon@jhon-legaltech.com*
- Red Profesional: ***LinkedIn***
- *Domicilio Digital:* **www.jhon-legaltech.com**