Comentarios al Nuevo proyecto de Reglamento de la Ley 31814, Ley que promueve el Uso de la Inteligencia Artificial en favor del desarrollo económico y social del país

El presente documento, preparado por la Iniciativa Tech & Law de la carrera de Derecho de la Universidad Científica del Sur, tiene por objetivo remitir comentarios al Reglamento de la ley N° 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país.

Artículo	Dice	Propuesta de modificación	Comentario
3.g	3.g) Inteligencia Artificial: Tecnología emergente de propósito general que tiene el potencial de mejorar el bienestar de las personas, contribuir a una actividad económica global sostenible positiva, aumentar la innovación y la productividad , y ayudar a responder a los desafíos globales clave. Inteligencia Artificial, adicionalmente es, la disciplina científica que busca crear programas informáticos (software), que ejecuten operaciones	**Artículo 3.g - Inteligencia Artificial: Sistema computacional que implementa modelos matemáticos y algoritmos diseñados para realizar tareas que convencionalmente requieren capacidades cognitivas humanas, caracterizado por capacidades fundamentales como el aprendizaje automático a partir de datos, el procesamiento y generación de lenguaje natural, el reconocimiento y clasificación de patrones, la optimización y toma de decisiones basada en datos, y la adaptación dentro de parámetros predefinidos. Estos sistemas operan con limitaciones inherentes que incluyen el**	La definición de Inteligencia Artificial propuesta en el artículo 3.g del reglamento presenta algunas limitaciones que requieren una reformulación sustancial. La actual redacción mezcla inadecuadamente el concepto técnico de IA con aspiraciones de política pública, creando ambigüedad en su interpretación y dificultando su aplicación práctica. El problema fundamental radica en que la definición actual no distingue entre IA débil (sistemas diseñados para tareas específicas) e IA fuerte (sistemas con capacidades generales similares a las humanas). Esta distinción es crucial para establecer marcos regulatorios apropiados según el tipo y alcance de la tecnología implementada. Además, la definición carece de precisión técnica al no especificar las capacidades y limitaciones concretas de los sistemas de IA. Una definición más precisa y técnicamente más coherente debería establecer que la Inteligencia Artificial es un sistema computacional que implementa modelos matemáticos y algoritmos diseñados para realizar tareas específicas que tradicionalmente requieren capacidades cognitivas humanas. Este sistema debe caracterizarse por capacidades fundamentales como el aprendizaje automático a partir de datos, el procesamiento y generación de lenguaje natural, el reconocimiento y clasificación de

	comparables a las que realiza la mente humana, como el aprendizaje o razonamiento lógico	**funcionamiento restringido a dominios específicos predefinidos, la dependencia de datos de entrenamiento, el requerimiento de supervisión humana y restricciones computacionales definidas. Todo sistema de IA debe presentar características técnicas verificables como una arquitectura algorítmica documentada, métricas de rendimiento cuantificables, trazabilidad de decisiones y capacidad de actualización controlada, operando en dominios específicos y predefinidos con capacidades de aprendizaje y adaptación limitadas a sus parámetros de diseño, siendo su rendimiento sujeto a evaluación y validación continua con resultados verificables y auditables.**	patrones, la optimización y toma de decisiones basada en datos, y la capacidad de adaptación dentro de parámetros predefinidos. Es fundamental, también, reconocer las limitaciones específicas de estos sistemas, eso incluye entender su dominio acotado de aplicación, la dependencia de datos de entrenamiento, la necesidad de supervisión humana y las restricciones computacionales definidas. Asimismo, es necesario especificar ciertas características técnicas verificables como la arquitectura algorítmica, las métricas de rendimiento cuantificables, la trazabilidad de decisiones y la capacidad de actualización controlada. Tomando en cuenta los argumentos anteriores, la definición debería enfatizar que estos sistemas operan dentro de dominios específicos y predefinidos, con capacidades de aprendizaje y adaptación limitadas a sus parámetros de diseño. Esto permitiría una regulación más efectiva y realista, basada en las capacidades reales de la tecnología actual, en lugar de conceptos aspiracionales o especulativos. Esta reformulación proporcionaría un marco regulatorio más claro y técnicamente preciso, facilitando tanto la implementación como la supervisión de sistemas de IA en el contexto peruano. Permitiría además una mejor evaluación de riesgos y establecimiento de medidas de control apropiadas según el tipo y capacidades específicas de cada sistema.
	Conceptos clave faltantes en la lista de definiciones	**SESGO ALGORÍTMICO: Distorsión sistemática en el procesamiento de**	El sesgo algorítmico, concepto fundamental ausente en el reglamento, debe entenderse como la presencia de errores sistemáticos en el procesamiento de datos que pueden

		datos o en el funcionamiento de sistemas de inteligencia artificial que produce resultados parcializados o discriminatorios, ya sea por sesgos preexistentes en los datos de entrenamiento o por aspectos técnicos del diseño y desarrollo del sistema, que pueden afectar de manera desproporcionada a determinados grupos o individuos. Esta distorsión puede manifestarse en forma de discriminación directa o indirecta, requiriendo mecanismos específicos de identificación, evaluación y mitigación. **EXPLICABILIDAD: Capacidad de un sistema de inteligencia artificial para presentar y justificar sus decisiones, predicciones o recomendaciones de manera comprensible para el usuario humano, incluyendo la descripción de la lógica subyacente, los datos utilizados y los factores determinantes en**	generar resultados injustos o discriminatorios. Su definición debe abarcar tanto los sesgos históricos presentes en los datos de entrenamiento como los sesgos técnicos introducidos durante el desarrollo del sistema. Resulta crucial establecer mecanismos específicos para su identificación y mitigación, especialmente considerando su impacto en grupos vulnerables. La explicabilidad, otro concepto esencial omitido, requiere una definición que enfatice la capacidad del sistema para presentar sus decisiones de manera comprensible para los usuarios humanos. Esto implica no solo la transparencia en la lógica utilizada sino también en los datos empleados para el entrenamiento y la toma de decisiones. Los niveles de explicabilidad deben ajustarse según el nivel de riesgo del sistema, estableciendo requisitos más estrictos para aplicaciones de alto impacto. La transparencia algorítmica debe definirse en términos de accesibilidad y comprensibilidad del funcionamiento del sistema. Esta definición necesita equilibrar la necesidad de transparencia con la protección de secretos comerciales legítimos, estableciendo niveles diferenciados de acceso a la información según el tipo de usuario y el contexto de aplicación. La trazabilidad emerge como otro concepto crucial que requiere definición precisa. Debe entenderse como la capacidad de rastrear y documentar cada paso en el proceso de toma de decisiones, incluyendo el mantenimiento de registros detallados sobre el entrenamiento del sistema, las actualizaciones realizadas y las decisiones tomadas. Los requisitos de trazabilidad deben especificar períodos mínimos de conservación de datos y estándares de documentación. La robustez y reproducibilidad son conceptos técnicos fundamentales que necesitan definiciones claras. La robustez

		cada resultado. Esta capacidad debe adaptarse al nivel de riesgo del sistema y al perfil del usuario, garantizando que las decisiones críticas sean especialmente transparentes y comprensibles. **TRANSPARENCIA ALGORÍTMICA: Cualidad de un sistema de inteligencia artificial que permite el acceso y comprensión de su funcionamiento, incluyendo la arquitectura del sistema, los datos utilizados y los procesos de toma de decisiones, sin comprometer la protección de secretos comerciales legítimos. El nivel de transparencia debe graduarse según el contexto de aplicación y el perfil del usuario, garantizando siempre un mínimo de información necesaria para la comprensión del sistema.** **TRAZABILIDAD: Capacidad de un sistema de inteligencia artificial para registrar, documentar y permitir el seguimiento de**	debe enfocarse en la capacidad del sistema para mantener su funcionamiento confiable bajo diferentes condiciones, mientras que la reproducibilidad debe garantizar la consistencia de resultados bajo condiciones idénticas. Ambos conceptos requieren criterios específicos de evaluación y protocolos de verificación. La supervisión humana, elemento crítico en sistemas de IA, debe definirse estableciendo niveles específicos de intervención humana requerida según el riesgo de la aplicación. Esta definición debe incluir las cualificaciones necesarias para los supervisores y protocolos claros de intervención en casos de funcionamiento inadecuado del sistema. La interoperabilidad y auditabilidad son conceptos que requieren definiciones técnicas precisas. La interoperabilidad debe enfocarse en la capacidad de los sistemas para intercambiar información de manera segura y efectiva, mientras que la auditabilidad debe garantizar la posibilidad de evaluación independiente del sistema. La responsabilidad algorítmica necesita una definición que establezca claramente la cadena de responsabilidad en el desarrollo y uso de sistemas de IA, incluyendo mecanismos específicos de compensación en casos de daños causados por el sistema.

		todas las etapas de su funcionamiento, incluyendo el proceso de desarrollo, entrenamiento, implementación y operación. Este registro debe incluir la documentación detallada de las decisiones tomadas, las actualizaciones realizadas y los datos utilizados, manteniendo esta información por un período mínimo establecido según el nivel de riesgo del sistema. **ROBUSTEZ Y REPRODUCIBILIDAD: La robustez se define como la capacidad del sistema para mantener un funcionamiento estable y confiable bajo diferentes condiciones de operación, resistiendo perturbaciones y manteniendo su rendimiento dentro de parámetros aceptables. La reproducibilidad se refiere a la capacidad del sistema para generar resultados consistentes cuando opera bajo condiciones idénticas, permitiendo la verificación independiente de**	

		su funcionamiento. **SUPERVISIÓN HUMANA: Proceso de control y vigilancia ejercido por personas cualificadas sobre el funcionamiento de sistemas de inteligencia artificial, cuyo nivel de intervención se determina según el riesgo y criticidad del sistema. Incluye la capacidad de monitoreo, intervención y anulación de decisiones del sistema cuando sea necesario, requiriendo cualificaciones específicas para los supervisores y protocolos establecidos de intervención.** **INTEROPERABILIDAD Y AUDITABILIDAD: La interoperabilidad es la capacidad de un sistema de inteligencia artificial para intercambiar información y operar de manera efectiva con otros sistemas o componentes, siguiendo estándares y protocolos establecidos. La auditabilidad es la cualidad que**	

		permite la evaluación independiente y sistemática del funcionamiento del sistema, incluyendo sus procesos, decisiones y resultados. **RESPONSABILIDAD ALGORÍTMICA: Marco que determina la atribución de responsabilidades en el desarrollo, implementación y uso de sistemas de inteligencia artificial, estableciendo obligaciones específicas para desarrolladores, implementadores y usuarios. Incluye mecanismos de compensación por daños causados por el sistema y requisitos de seguros o garantías según el nivel de riesgo de la aplicación.**	

2	Artículo 2. Ámbito de aplicación Las disposiciones del presente Reglamento son aplicables a: a) Las entidades establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de la Ley Nº 27444,	**Artículo 2. Ámbito de aplicación** **Las disposiciones del presente Reglamento son aplicables a todas las entidades establecidas en el artículo I del Título Preliminar del Texto Único Ordenado de**	El artículo 2 del reglamento, al definir su ámbito de aplicación, no aborda explícitamente cómo se aplicará la normativa a empresas que, sin tener presencia física en Perú, ofrecen servicios de IA a usuarios peruanos. Esta omisión genera incertidumbre jurídica, particularmente en la

	Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo Nº 004-2019-JUS u otra norma que lo sustituya. b) Las empresas que realizan actividad empresarial del Estado que se encuentran en el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE), así como las empresas públicas de los gobiernos regionales y locales. c) Conforme a lo dispuesto en el artículo 1 de la Ley, el presente Reglamento se aplica al uso de la Inteligencia Artificial, ya sea efectuado por las organizaciones de la sociedad civil, ciudadanos, academia y el sector privado que integran el Sistema Nacional de Transformación Digital.	**la Ley Nº 27444, Ley del Procedimiento Administrativo General, aprobado mediante Decreto Supremo Nº 004-2019-JUS u otra norma que lo sustituya, así como a las empresas que realizan actividad empresarial del Estado que se encuentran en el ámbito del Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado (FONAFE), empresas públicas de los gobiernos regionales y locales, y a las organizaciones de la sociedad civil, ciudadanos, academia y sector privado que integran el Sistema Nacional de Transformación Digital.** **El reglamento extiende su aplicación a los proveedores extranjeros de servicios de Inteligencia Artificial que ofrezcan servicios dirigidos a usuarios en territorio peruano, procesen datos de usuarios peruanos, generen efectos sustanciales en el mercado peruano o alcancen un umbral mínimo de usuarios activos en Perú. Esta aplicación incluye servicios de Inteligencia Artificial**	regulación de empresas multinacionales donde no se establecen criterios claros sobre su aplicación cuando estas procesan datos en múltiples jurisdicciones o utilizan sistemas de IA desarrollados fuera del territorio nacional. El procesamiento de datos fuera del territorio nacional constituye otro aspecto crítico insuficientemente regulado. El reglamento no especifica cómo se garantizará el cumplimiento de estándares peruanos cuando los datos son procesados en servidores ubicados en otros países, ni establece mecanismos para asegurar la protección de datos personales en estos casos. Esta falta de claridad podría resultar en vacíos regulatorios significativos. En tal sentido, consideramos necesario establecer un criterio de efecto sustancial que aplique el reglamento a todo servicio de IA dirigido a usuarios en Perú. Esto implica establecer umbrales cuantitativos para determinar la significancia del impacto y definir indicadores precisos para medir el efecto en el mercado peruano. La vinculación efectiva debe determinarse mediante criterios específicos que establezcan cuándo existe conexión suficiente con Perú, incluyendo requisitos de registro para proveedores extranjeros y obligaciones específicas según el nivel de vinculación. Esto debe

		que, independientemente de su ubicación física, impacten significativamente en derechos fundamentales de ciudadanos peruanos, afecten sectores críticos de la economía nacional, involucren procesamiento de datos sensibles de ciudadanos peruanos o presten servicios esenciales a población vulnerable. **La vinculación efectiva con Perú se determinará considerando el número de usuarios peruanos activos, el volumen de datos procesados de ciudadanos peruanos, el impacto económico en el mercado nacional, el nivel de riesgo de la aplicación de Inteligencia Artificial y el sector de aplicación del servicio.** **Los proveedores extranjeros deberán designar un representante legal en Perú, registrarse ante la autoridad competente, establecer mecanismos de atención al usuario en Perú y someterse a la jurisdicción peruana para efectos de supervisión y fiscalización. Para el**	complementarse con mecanismos robustos de cooperación internacional, incluyendo protocolos de intercambio de información y procedimientos coordinados de supervisión. En materia de protección de datos transfronterizos, el reglamento debe establecer requisitos específicos para las transferencias internacionales de datos, definiendo estándares mínimos de protección y mecanismos de verificación de cumplimiento. La responsabilidad legal en operaciones transnacionales debe quedar claramente definida, estableciendo requisitos de representación legal en Perú y mecanismos efectivos para la ejecución de decisiones regulatorias. La implementación de estas mejoras requerirá el desarrollo de capacidades técnicas de supervisión, el establecimiento de acuerdos internacionales de cooperación y la creación de mecanismos de monitoreo transfronterizo. Es fundamental que el personal regulador reciba formación especializada para manejar la complejidad de las operaciones transnacionales en el ámbito de la IA.

		procesamiento transfronterizo de datos, se requiere cumplir estándares mínimos de protección equivalentes a la normativa peruana, implementar mecanismos de trazabilidad y auditoría, garantizar el acceso de autoridades supervisoras a la información relevante y establecer protocolos de seguridad y confidencialidad. **La autoridad competente establecerá mecanismos de cooperación internacional para la supervisión efectiva, protocolos de intercambio de información con autoridades extranjeras, procedimientos coordinados de fiscalización y sistemas de monitoreo transfronterizo. El incumplimiento de estas disposiciones conllevará restricciones de acceso al mercado peruano, sanciones administrativas según la normativa vigente, obligaciones de reparación por daños causados y otras medidas que determine la autoridad**	

		competente.	

	Limitaciones a considerar: propuesta de artículos nuevos	**CAPÍTULO [X] REQUISITOS TÉCNICOS Y ESTÁNDARES DE CALIDAD** **Artículo [XX]. Requisitos Técnicos Fundamentales** **1. Precisión y Exactitud: Los sistemas de Inteligencia Artificial deberán cumplir con niveles mínimos de precisión según su ámbito de aplicación: a) Sistemas de alto riesgo en salud: precisión mínima del 99% b) Sistemas financieros críticos: margen de error máximo del 0.01% c) Sistemas de seguridad: tasa de falsos positivos inferior al 0.1% d) Otros sistemas: niveles de precisión acordes a estándares internacionales según su**	En cuanto a los aspectos técnicos, el reglamento carece de especificaciones sobre niveles mínimos de precisión y exactitud necesarios para diferentes tipos de aplicaciones de IA. Esta omisión es particularmente crítica en sectores sensibles como salud, finanzas y seguridad, donde la precisión del sistema puede tener consecuencias significativas. Es necesario establecer umbrales mínimos aceptables y métricas estandarizadas para la evaluación del rendimiento, junto con protocolos específicos de medición y verificación. Las métricas de calidad de datos representan otro aspecto técnico insuficientemente desarrollado. El reglamento debe establecer estándares claros de completitud y representatividad de datos, incluyendo criterios específicos para su actualización y vigencia. Es fundamental incorporar protocolos detallados de limpieza y preparación de datos, así como requisitos rigurosos para la documentación de fuentes y medidas de control de sesgos. La documentación técnica requiere una especificación más detallada, estableciendo una estructura y contenido mínimo requerido. Esto

		sector **2. Calidad de Datos: Todo sistema de Inteligencia Artificial debe cumplir con los siguientes requisitos de calidad de datos: a) Completitud mínima del 95% en variables críticas b) Actualización de datos según la criticidad del sistema:** **○ Sistemas de alto riesgo: actualización mensual** **○ Sistemas de riesgo medio: actualización trimestral** **○ Sistemas de bajo riesgo: actualización anual c) Documentación completa de fuentes y metodologías**	debería incluir especificaciones completas de la arquitectura del sistema, documentación exhaustiva de algoritmos y modelos utilizados, un registro detallado de cambios y actualizaciones, así como documentación de incidentes y problemas encontrados durante la operación del sistema. Los requisitos de pruebas constituyen otro elemento crítico ausente en el reglamento. Es necesario establecer protocolos específicos para pruebas unitarias, pruebas de integración, evaluaciones de stress y rendimiento, así como pruebas exhaustivas para la detección y eliminación de sesgos. Adicionalmente, se deben incluir pruebas de seguridad robustas para garantizar la integridad del sistema. Respecto al marco regulatorio, el reglamento debe fortalecer su alineación con estándares internacionales, particularmente con las regulaciones de la Unión Europea sobre IA, los estándares de la OCDE y los principios IEEE para IA ética. Es fundamental incorporar referencias específicas a estándares ISO/IEC relevantes, como el ISO/IEC 42001 para Sistemas de Gestión de IA, el ISO/IEC 23053 para Frameworks de IA, y el ISO/IEC 38507 para Gobernanza de IA. La compatibilidad con regulaciones sectoriales

		de recolección d) Protocolos verificables de limpieza y preparación de datos **3. Documentación Técnica: Los sistemas deberán mantener documentación técnica que incluya: a) Arquitectura detallada del sistema b) Especificaciones completas de algoritmos y modelos c) Registro de cambios y actualizaciones d) Documentación de incidentes y soluciones e) Métricas de rendimiento y evaluaciones de calidad** **4. Requisitos de Pruebas: Todo sistema debe someterse a: a) Pruebas unitarias de componentes b) Pruebas de integración del sistema c) Evaluaciones de stress y rendimiento d) Pruebas de detección de**	existentes requiere especial atención. El reglamento debe articularse efectivamente con la normativa financiera de la SBS, las regulaciones de salud del MINSA, la normativa de telecomunicaciones del MTC y las disposiciones de protección al consumidor de INDECOPI. Esta articulación debe garantizar coherencia regulatoria mientras se mantienen los estándares específicos necesarios para cada sector. La coordinación institucional es un aspecto que necesita mayor desarrollo. El reglamento debiera establecer mecanismos claros de colaboración entre las diferentes autoridades competentes, definiendo procedimientos específicos para la supervisión conjunta y protocolos eficientes para el intercambio de información entre instituciones. Estas mejoras necesitan el desarrollo de anexos técnicos detallados que complementen el reglamento principal, la creación de comités técnicos especializados que supervisen su implementación, y la creación de mecanismos de actualización periódica que permitan mantener el marco regulatorio al día con los avances tecnológicos. Asimismo, se requiere implementar sistemas robustos de monitoreo y evaluación para asegurar el cumplimiento efectivo de las disposiciones técnicas y regulatorias.

		sesgos e) Auditorías de seguridad periódicas **Artículo [XY]. Alineación con Estándares Internacionales** **1. Cumplimiento de Normas: Los sistemas deberán cumplir con: a) Estándares ISO/IEC aplicables b) Regulaciones de IA de la Unión Europea c) Principios OCDE para IA d) Estándares IEEE para IA ética** **2. Articulación Sectorial: Las implementaciones deberán considerar: a) Normativa financiera de la SBS b) Regulaciones de salud del MINSA c) Normativa de telecomunicaciones del MTC d) Disposiciones de INDECOPI** **Artículo [XZ]. Coordinación y Supervisión** **1. Mecanismos de Coordinación: Se establecen los**	

		siguientes: a) Comité Técnico Intersectorial de IA b) Sistema de Supervisión Integrada c) Protocolo de Intercambio de Información d) Mecanismos de Actualización Normativa 2. Evaluación y Monitoreo: Se implementará: a) Sistema de Monitoreo Continuo b) Evaluaciones Periódicas de Cumplimiento c) Auditorías Técnicas Independientes d) Mecanismos de Retroalimentación y Mejora 3. Actualización y Vigencia: El marco técnico será revisado: a) Anualmente para ajustes menores b) Cada tres años para actualizaciones mayores c) Inmediatamente ante avances tecnológicos significativos 4. Anexos Técnicos: Se desarrollarán anexos específicos	

		para: a) Protocolos detallados de pruebas b) Especificaciones técnicas por sector c) Guías de implementación d) Metodologías de evaluación	

Capitulo III. Subcapítulo I. Gestión de riesgos		**artículos adicionales para el Subcapítulo I sobre Gestión de Riesgos:** **Artículo [X]. Criterios de Evaluación de Riesgos La evaluación de riesgos de sistemas de Inteligencia Artificial se realizará considerando criterios cuantitativos y cualitativos específicos. El impacto en derechos fundamentales se medirá mediante un criterio de severidad en escala del 1 al 5, considerando el alcance poblacional afectado, la duración del impacto y la reversibilidad de los efectos. Las métricas de evaluación por nivel establecerán como riesgo inaceptable aquel que presente un impacto crítico en derechos fundamentales (severidad 5), riesgo**	El capítulo sobre gestión de riesgos en el uso de inteligencia artificial de la propuesta de reglamento presenta varios aspectos positivos que merecen destacarse, aunque también exhibe algunas limitaciones importantes que requieren atención. En cuanto a los aspectos positivos, el reglamento establece una clasificación clara y sistemática de los riesgos, dividiéndolos en categorías que van desde inaceptable hasta bajo. Esta categorización se alinea con las tendencias internacionales en regulación basada en riesgos y permite un enfoque proporcionado según el nivel de riesgo identificado. También resulta positivo que se haya establecido un marco institucional definido, asignando roles específicos a diferentes entidades como la PCM, INDECOPI y CONCYTEC, lo que proporciona claridad en la supervisión y control. Es particularmente destacable el

		alto para impacto significativo (severidad 4), riesgo medio para impacto moderado (severidad 2-3), y riesgo bajo para impacto mínimo (severidad 1). Los factores sectoriales específicos establecerán para el sector salud un margen de error máximo de 0.1%, para el sector financiero una precisión mínima de 99.9%, para el sector justicia la trazabilidad completa de decisiones, y para el sector educación la transparencia total de criterios. **Artículo [Y]. Procedimientos de Supervisión y Control Los mecanismos de supervisión incluirán auditorías técnicas trimestrales, evaluaciones de impacto semestrales, monitoreo continuo automatizado y reportes periódicos obligatorios. Los recursos y capacidades requeridos comprenderán personal técnico especializado, infraestructura de evaluación, herramientas de monitoreo y presupuesto específico asignado. La coordinación interinstitucional se realizará a través de**	tratamiento detallado de los riesgos inaceptables, donde el reglamento prohíbe explícitamente usos que podrían afectar derechos fundamentales, como la manipulación del comportamiento y la discriminación. En cuanto a los riesgos altos, el reglamento identifica acertadamente sectores críticos como salud, educación y justicia, estableciendo obligaciones específicas para estos casos. Sin embargo, el reglamento presenta también importantes limitaciones. Una de las principales críticas es la falta de precisión en las definiciones y criterios para evaluar los niveles de riesgo. Si bien se establecen categorías generales, no se proporcionan criterios cuantitativos o métricas específicas que permitan una evaluación objetiva y consistente. Esta ambigüedad podría generar dificultades en la implementación práctica y potenciales inconsistencias en la clasificación de riesgos. Los mecanismos de supervisión y control también presentan debilidades. Aunque se establecen entidades responsables, no se especifican claramente los recursos y capacidades necesarias para realizar una supervisión efectiva. Además, existe una potencial superposición de competencias entre las diferentes entidades supervisoras, sin que se establezcan mecanismos claros

		un Comité Técnico de Supervisión, con protocolos de comunicación establecidos, un sistema integrado de información y mecanismos de respuesta rápida. **Artículo [Z]. Plazos y Actualización Las evaluaciones periódicas incluirán una evaluación inicial previa al despliegue, evaluación continua mensual para sistemas de alto riesgo, semestral para riesgo medio y anual para riesgo bajo. La actualización de criterios contemplará una revisión anual de parámetros, actualización tecnológica bianual, ajuste inmediato ante nuevos riesgos identificados y consulta pública previa a cambios significativos. La documentación y registro mantendrá una historia completa de evaluaciones, registro de actualizaciones, documentación de incidentes y medidas correctivas implementadas.** **Artículo [W]. Responsabilidades y Sanciones La asignación de responsabilidades establecerá**	de coordinación entre ellas. En términos de implementación, el reglamento presenta algunos vacíos importantes. No se establecen plazos específicos para las evaluaciones de riesgo, ni se proporcionan guías detalladas para la clasificación de riesgos. También falta un mecanismo claro para la actualización de criterios conforme evolucione la tecnología y surjan nuevos riesgos. La asignación de responsabilidades también presenta áreas de mejora. Se observa una posible superposición de funciones entre diferentes entidades supervisoras, y no se establecen claramente los mecanismos de coordinación. Además, el reglamento no especifica las sanciones por incumplimiento, lo que podría debilitar su capacidad de enforcement. Para fortalecer el marco regulatorio, sería recomendable desarrollar guías técnicas detalladas que complementen el reglamento, establecer criterios cuantitativos de evaluación y definir procedimientos específicos de supervisión. También es crucial fortalecer las capacidades técnicas de las entidades supervisoras y establecer mecanismos claros de coordinación entre ellas. En el aspecto procedimental, es necesario desarrollar protocolos detallados de evaluación, establecer plazos específicos para el cumplimiento y crear

		obligaciones específicas para desarrolladores en cuanto al diseño seguro, implementadores respecto al despliegue responsable, supervisores para el control efectivo y usuarios en relación al uso adecuado. El régimen sancionador contemplará infracciones leves sancionadas hasta con 50 UIT, infracciones graves hasta 150 UIT, e infracciones muy graves hasta 500 UIT, además de medidas correctivas obligatorias. Los procedimientos de apelación considerarán como primera instancia la autoridad sectorial, segunda instancia el comité técnico y como instancia final un tribunal especializado. **Artículo [V]. Protección de Derechos Los mecanismos de protección incluirán un sistema de alertas tempranas, canal de denuncias, medidas cautelares y procedimientos de reparación de daños. El monitoreo continuo se realizará mediante un sistema automatizado de supervisión, con indicadores de desempeño, alertas**	mecanismos de actualización periódica que permitan adaptar la regulación a los cambios tecnológicos. Asimismo, es importante fortalecer los mecanismos de protección de derechos, establecer procedimientos de apelación claros y crear sistemas de monitoreo continuo.

		de desviaciones y reportes periódicos. La transparencia y rendición de cuentas se garantizará a través de informes públicos trimestrales, un portal de transparencia, mecanismos de consulta ciudadana y audiencias públicas anuales.	
Subcapítulo II. privacidad y transparencia		**UBCAPÍTULO II MEDIDAS EN MATERIA DE PRIVACIDAD Y TRANSPARENCIA** **Artículo 21. Protocolos Específicos de Protección de Datos Los sistemas de Inteligencia Artificial deberán implementar protocolos específicos de protección que garanticen la privacidad y seguridad de los datos personales. Las medidas técnicas de protección incluirán cifrado de extremo a extremo, anonimización irreversible de datos sensibles, segregación de datos personales, controles de acceso multinivel y registro detallado de operaciones de procesamiento. Es obligatoria la**	En cuanto a la protección de la privacidad, de lo cual se ocupa el Subcapítulo II de la propuesta de reglamento, observamos que establece un vínculo directo con la normativa vigente sobre protección de datos personales, lo cual proporciona un marco legal de referencia. Sin embargo, la redacción resulta demasiado general y carece de medidas concretas de protección. Es notable la ausencia de mecanismos específicos para la protección de datos en sistemas de IA, especialmente considerando los riesgos únicos que presenta esta tecnología. En el ámbito de la transparencia de la información, el reglamento introduce elementos positivos como la obligación de mantener informados a los ciudadanos y la promoción del uso de software libre, incluyendo la disposición de compartir desarrollos a través del Portal de Software Público Peruano. No obstante, estas

		realización de evaluaciones de impacto en la privacidad que comprendan análisis previo al despliegue, evaluaciones periódicas de riesgo, medidas de mitigación documentadas, auditorías independientes anuales y actualización continua de medidas de protección. Los sistemas deberán cumplir con requisitos mínimos de seguridad que incluyan autenticación multifactor obligatoria, sistemas de detección de intrusiones, protocolos de respuesta a incidentes, copias de seguridad cifradas y planes de continuidad documentados. **Artículo 22. Transparencia y Explicabilidad Algorítmica Todo sistema de Inteligencia Artificial deberá proporcionar información detallada sobre su funcionamiento, incluyendo los criterios de toma de decisiones, fuentes de datos utilizadas, limitaciones y sesgos conocidos, así como las medidas de mitigación**	disposiciones carecen de especificidad en cuanto al nivel de detalle de la información que debe proporcionarse, los formatos o estándares para la transparencia, y los plazos para la actualización de información. Una crítica fundamental es la insuficiencia normativa del subcapítulo, que resulta demasiado breve y general para la importancia de la materia que regula. No se desarrollan aspectos críticos como las auditorías de transparencia ni se establece regulación específica sobre algoritmos y toma de decisiones automatizada. Esta brevedad genera vacíos regulatorios significativos, particularmente en lo referente al derecho a explicación de decisiones automatizadas, la regulación de sesgos algorítmicos y los mecanismos de rendición de cuentas. Los aspectos procedimentales también presentan deficiencias notables. No se establecen procedimientos claros para las solicitudes de información, faltan mecanismos de verificación de cumplimiento y no se especifican sanciones por incumplimiento. Estas omisiones podrían dificultar la implementación efectiva de las disposiciones del reglamento. Para fortalecer el marco regulatorio, sería necesario desarrollar protocolos específicos de protección de datos para sistemas de IA, establecer requisitos mínimos

		implementadas. Las decisiones automatizadas deberán incluir justificación individualizada, factores determinantes, alternativas consideradas y mecanismos de rectificación. La documentación técnica deberá presentarse en formatos estandarizados que incluyan reportes periódicos de desempeño, registros de actualizaciones, informes de auditoría y evaluaciones de impacto. **Artículo 23. Auditorías y Verificación de Cumplimiento Los sistemas de Inteligencia Artificial estarán sujetos a auditorías periódicas de transparencia que incluyan evaluaciones técnicas independientes, verificación de sesgos algorítmicos, análisis de impacto social y validación de resultados. Las auditorías serán realizadas por entidades independientes acreditadas y deberán ejecutarse al menos una vez al año o cuando se realicen modificaciones**	de seguridad y definir procesos de evaluación de impacto en la privacidad. En materia de transparencia, es crucial establecer niveles mínimos de información a proporcionar, desarrollar formatos estandarizados de reporte y crear mecanismos de verificación independiente. Los aspectos institucionales también requieren atención. Es necesario fortalecer el rol de las autoridades supervisoras, establecer mecanismos efectivos de coordinación interinstitucional y desarrollar las capacidades técnicas necesarias para una supervisión efectiva. La implementación del reglamento necesita plazos claros para el cumplimiento, guías técnicas detalladas y sistemas robustos de monitoreo y evaluación. A pesar de estas limitaciones, el subcapítulo establece principios básicos importantes y reconoce la relevancia de la transparencia y la promoción del software libre. Sin embargo, el marco regulatorio resulta insuficiente, con falta de especificidad en medidas y procedimientos, y ausencia de mecanismos efectivos de enforcement.

		sustanciales al sistema. Los resultados de las auditorías serán públicos y accesibles a través del Portal de Software Público Peruano. **Artículo 24. Sistema de Solicitudes y Reclamos Se establece un sistema unificado de solicitudes y reclamos relacionados con sistemas de Inteligencia Artificial, que deberá incluir canales de acceso definidos, plazos de respuesta máximos de 30 días hábiles, formatos estandarizados y mecanismos de seguimiento. Las solicitudes de información deberán ser atendidas de manera gratuita y en lenguaje comprensible para el ciudadano. El sistema incluirá un proceso de apelación ante la autoridad competente cuando la respuesta sea insatisfactoria.** **Artículo 25. Régimen Sancionador Específico El incumplimiento de las disposiciones en materia de privacidad y transparencia será sancionado según la siguiente escala: a) Infracciones leves:**	

		multa de 1 a 50 UIT b) Infracciones graves: multa de 51 a 150 UIT c) Infracciones muy graves: multa de 151 a 500 UIT Las sanciones serán aplicadas sin perjuicio de la responsabilidad civil o penal que corresponda y la obligación de implementar medidas correctivas. **Artículo 26. Supervisión y Coordinación Institucional La supervisión del cumplimiento de estas disposiciones será realizada de manera coordinada entre la Autoridad Nacional de Protección de Datos Personales, la Secretaría de Gobierno Digital y las autoridades sectoriales competentes. Se establece un Comité Técnico de Supervisión que coordinará las acciones de control y establecerá criterios uniformes de evaluación. Las autoridades supervisoras deberán contar con personal especializado y recursos técnicos adecuados para el cumplimiento de sus funciones.** **Artículo 27.**	

		Implementación y Monitoreo Continuo La implementación de estas disposiciones seguirá un cronograma gradual que incluye: a) Fase de adecuación: 6 meses desde la publicación del reglamento b) Implementación completa: 12 meses desde la publicación c) Evaluaciones periódicas: trimestrales d) Actualizaciones de protocolos: anuales La Secretaría de Gobierno Digital establecerá un sistema de monitoreo continuo que incluirá indicadores de cumplimiento, métricas de desempeño y mecanismos de alerta temprana.	

Elaborado por: Olga Alcantara Francia - Lider de la iniciativa de Tech & Law de la carrera de Derecho de la Universidad Científica del Sur.