

## VI Congreso ISACA Iberoamérica

*Del 26 al 28 de mayo de 2026. Formato virtual*

### IA Y RIESGOS DIGITALES

Gobernar lo inesperado, proteger lo esencial.



# Gobernanza digital y riesgos de la IA según la legislación brasileña: impactos y desafíos en aplicaciones y casos de estudio

*Adriano Neves, Ph.D, CRISC, CGEIT, CDPSE, CSM*

## **Adriano Neves, Ph.D, CGEIT, CRISC, CPDSE, PMP, CSM**

- **Ph.D in Information Systems - USP (University of Sao Paulo) – Research in IT Governance;**
- **Master Degree in Computer Engineering – IPT / USP;**
- **Certifications in CGEIT, CRISC and CDPSE – ISACA;**
- **Project Management Professional (PMP®) pelo PMI;**
- **Scrum Master Certification (Scrum Alliance);**
- **Accredited Instructor BlockChain (EXIN);**
- **Accredited Instructor ITIL (EXIN);**
- **Executive Advisory of ISACA São Paulo Chapter;**
- **Digital Trust Director - Real Project Consulting & Training;**
- **CAIO (Chief Artificial Intelligence Officer) – MetaQualys Health – [www.metaqualys.com](http://www.metaqualys.com)**
- **Professor / Lecturer in IT MBA and Post Graduation Courses: FIA, FGV, ITA, FIAP, HSM, INSPER, PUC-RS e outros;**
- **More than 30 years of experience in Information Technology, IT Governance, IT Audit, IT Risk and Privacy;**
- **Experience as CTO, IT Executive, IT Audit, Compliance e IT Project Management: HP, Atos Origin, Diveo Datacenter and others.**



**ISACA**  
IBEROAMÉRICA



**LinkedIn**

Adriano Neves, Ph.D, PMP, CPDSE, CGEIT,  
CRISC, CSM  
Director, Digital Trust



# Cumplimiento normativo y supervisión de riesgos potenciales

La inteligencia artificial optimiza la verificación del cumplimiento normativo mediante el seguimiento constante de normativas cambiantes como:

- LGPD (Brasil)
- HIPAA (Estados Unidos);
- GDPR (Europa);
- **La Ley de IA de Brasil, UE, EUA.**

Los marcos de **gobernanza** para la IA admiten registros de auditoría en tiempo real, restricciones de acceso basadas en permisos y evaluaciones de riesgos automatizadas, lo que ayuda a las instituciones a mantener el cumplimiento normativo y a minimizar la carga de trabajo manual.



# LEGISLACIÓN BRASILEÑA DE IA



# CONTEXTO TECNOLÓGICO



## Aceleración y Necesidad

Brasil es uno de los mayores adoptantes de IA en América Latina, impulsando la urgencia de una gobernanza digital robusta.

Crecimiento exponencial en servicios financieros digitales.

Digitalización masiva del sistema de salud pública (SUS).

Desafíos éticos en el procesamiento de datos masivos.

# MARCO LEGAL BRASILEÑO

## El "Marco Legal de la IA"

El Proyecto de Ley 2338/2023 establece normas generales para el desarrollo, implementación y uso ético de la IA en Brasil.

Enfoque basado en derechos fundamentales.

Centralidad de la persona humana.

Promoción de la innovación responsable.



<https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>

# PRINCIPIOS RECTORES



## Transparencia

Deber de informar sobre la interacción con sistemas automatizados.



## No Discriminación

Mitigación activa de sesgos algorítmicos en la toma de decisiones.






## Supervisión

Garantía de intervención humana efectiva en el ciclo de vida de la IA.

# DERECHOS DEL CIUDADANO

## Empoderamiento del Usuario

La legislación brasileña es pionera en detallar los derechos de quienes son impactados por decisiones de IA.

-  Derecho a la explicación.
-  Derecho a la revisión humana.
-  Protección contra decisiones sesgadas.



# ENFOQUE BASADO EN RIESGO

## Niveles de Clasificación

Inspirado en el modelo europeo, el PL brasileño divide los sistemas según su impacto potencial.

**Riesgo Excesivo:** Prácticas prohibidas por violar derechos.

**Alto Riesgo:** Requiere evaluaciones estrictas (Salud, Finanzas).

**Bajo/Medio Riesgo:** Obligaciones de transparencia general.



# EL PILAR DEL CUMPLIMIENTO



## IA: Metodología GRC

Obligatoria para sistemas de **Alto Riesgo**. Debe documentar:

Descripción de la lógica del sistema.

Medidas de mitigación de riesgos y sesgos.

Pruebas de robustez y precisión.

Plan de gobernanza de datos.

---

# Comparativa Internacional

Brasil vs. Unión Europea (EU AI Act) vs. EE.UU. (NIST)

# CONVERGENCIA REGULATORIA

## Similitudes y Diferencias

El PL 2338/2023 bebe directamente del EU AI Act, pero adapta realidades locales.

**UE:** Enfoque regulatorio de mercado único y producto.

**Brasil:** Enfoque más centrado en derechos civiles y defensa del consumidor.

Ambos utilizan la clasificación basada en riesgos.



# MÉTRICAS DE GOBERNANZA

Criterio	Brasil (PL 2338)	UE (AI Act)	EE.UU. (Executive Order)
Enfoque Principal	Derechos Humanos	Mercado y Seguridad	Innovación y Riesgo
Supervisión Humana	Obligatoria (Alto Riesgo)	Obligatoria (Alto Riesgo)	Recomendada / Guías
Sandboxes	Previstos en Ley	Fomento Obligatorio	Enfoque Voluntario

# ANÁLISIS CRÍTICO: BRASIL

## Ventajas

Claridad jurídica para ciudadanos y protección contra abusos algorítmicos.

- + Fuerte protección de derechos.
- + Alineación con estándares globales.

## Desventajas

Riesgo de excesiva burocracia que frene a las Startups locales.

- Costos altos de cumplimiento.
- Incertidumbre sobre autoridad fiscalizadora.

# Derechos de las personas afectadas

## 04

### Direitos Centrais

Información: Saber que se está interactuando con IA.

Explicación: Comprender la lógica detrás de la decisión.

Intervención: Solicitar una revisión humana.

No discriminación: Corregir activamente los sesgos.



**La Ley General de Protección de Datos (LGPD), Ley n.º 13.709/2018, se promulgó para proteger los derechos fundamentales a la libertad y la privacidad, así como la libre formación de la personalidad de cada individuo. La Ley regula el tratamiento de datos personales, tanto en formato físico como digital, realizado por personas físicas o jurídicas en virtud del derecho público o privado, abarcando un amplio abanico de operaciones que pueden llevarse a cabo de forma manual o digital.**



# Estudio de caso en el sector de SALUD

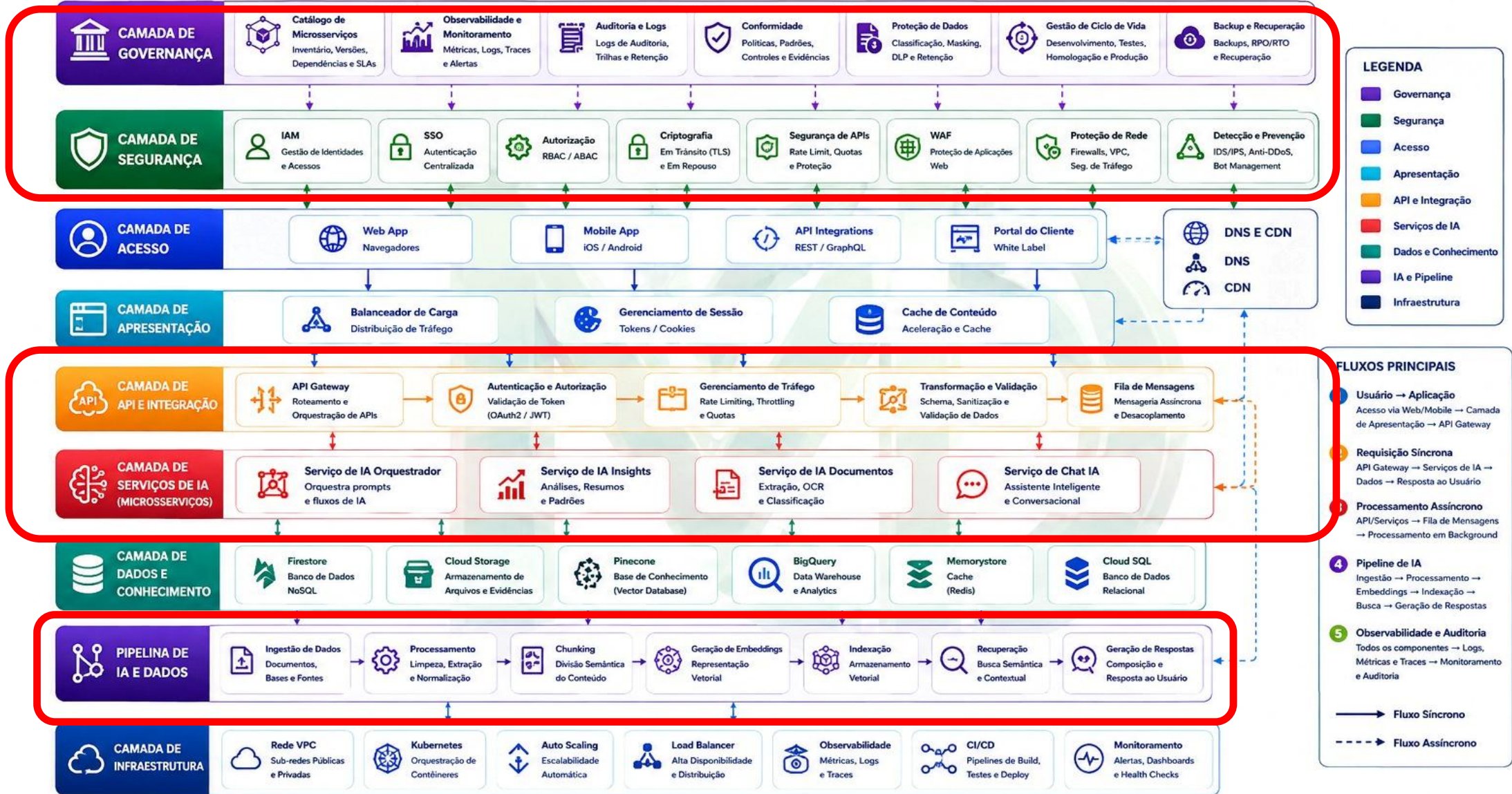


**Company: Brazilian HealthTec Startup**

**Project: Artificial Intelligence Diagnostic Imaging Platform (Machine Learning/AI)**

**Tools: Gemini 3.5 Pro / Microsoft Azure ML / Google Vertex AI**





**i** A Governança define políticas e padrões aplicáveis a todas as camadas e microserviços. A Segurança é aplicada transversalmente para proteger dados, acessos e comunicações.

# Software as a Medical Device



# Software as a Medical Device



**IMDRF** International Medical Device Regulators Forum

## SaMD Categories

IMDRF/AIML WG/N88 FINAL: 2025

**Good machine learning practice for medical device development: Guiding principles**

State of Healthcare situation or condition	Significance of information provided by SaMD to healthcare decision		
	Treat or diagnose	Drive clinical management	Inform clinical management
Critical	IV	III	II
Serious	III	II	I
Non-serious	II	I	I

Natureza da Informação / Gravidade da Condição	Não Grave	Grave	Crítica / Fatal
<b>Informar</b> (ex.: registrar dados)	Cat. I	Cat. I	Cat. II
<b>Direcionar</b> (ex.: apoiar diagnóstico)	Cat. I	Cat. II	Cat. III
<b>Diagnosticar/Tratar</b> (ex.: fechar diagnóstico automaticamente)	Cat. II	Cat. III	Cat. IV



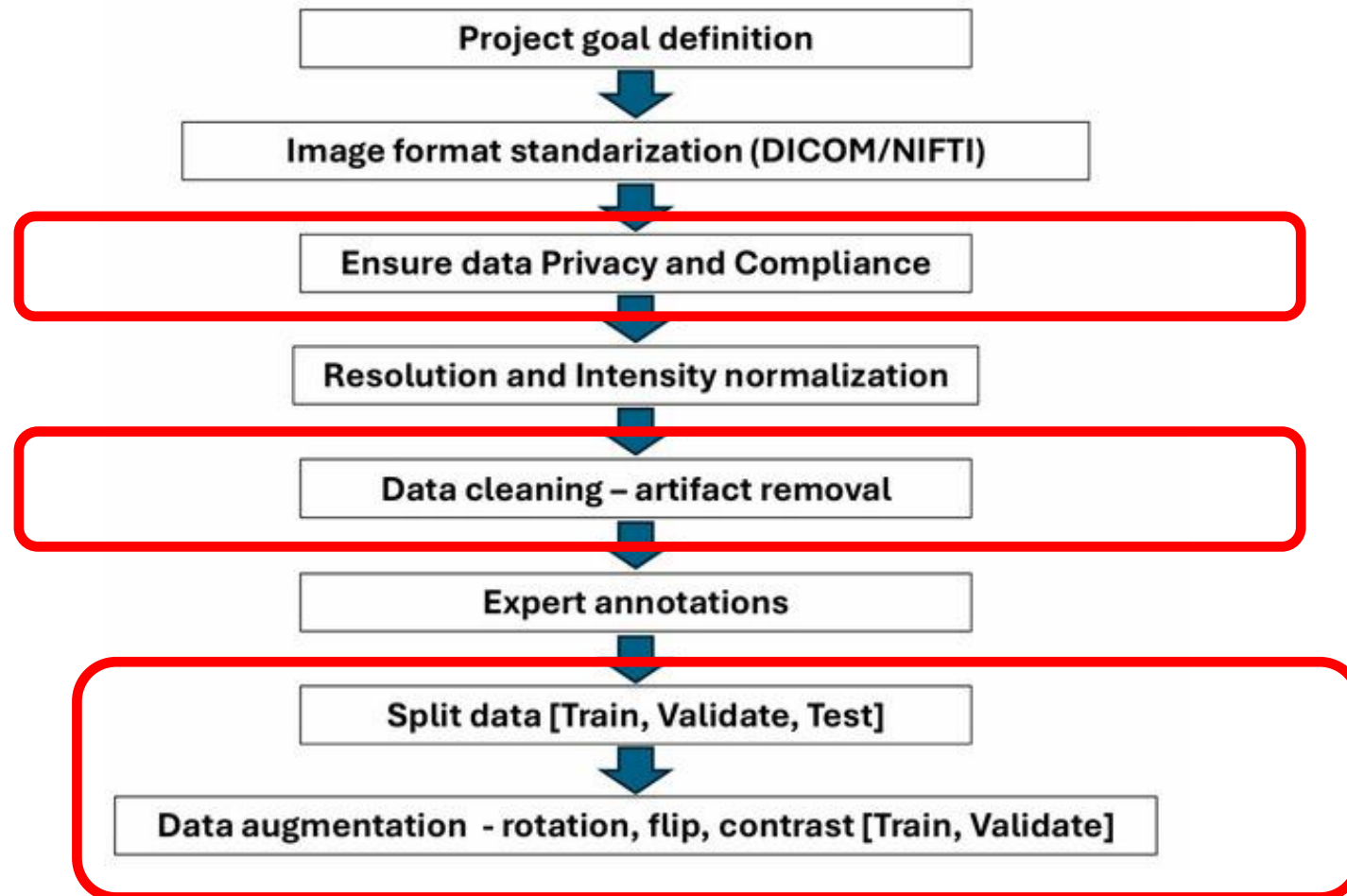
## Normas Técnicas Essenciais para Desenvolvimento de SaMD

O desenvolvimento de um SaMD aprovável exige conformidade com um conjunto de normas técnicas internacionais. As principais são:

<b>Norma</b>	<b>Escopo</b>	<b>Aplicação</b>
<b>IEC 62304</b>	Ciclo de vida de software médico	Obrigatória para SaMD Classes II–IV
<b>IEC 82304-1</b>	Segurança de produtos de software de saúde	Complementar à IEC 62304, foco em app independente
<b>ISO 14971</b>	Gerenciamento de riscos	Exigida em todas as classes, inclui riscos de IA
<b>ISO 13485</b>	Sistema de gestão da qualidade	Base para o CBPF exigido nas classes III–IV
<b>IEC 81001-5-1</b>	Cibersegurança em software de saúde	Crescente exigência em mercados globais

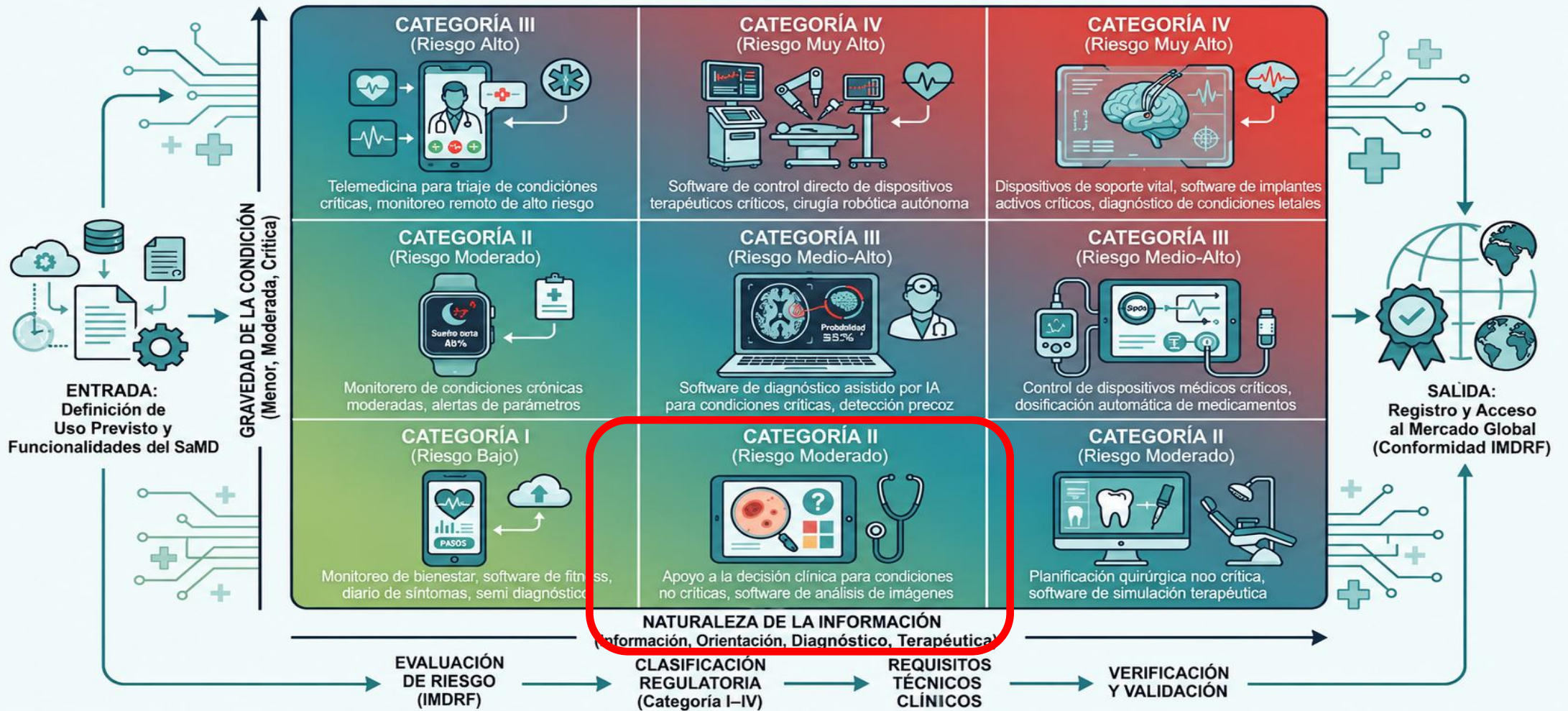
# Software as a Medical Device

## Artificial Intelligence Diagnostic Imaging Platform



# Software as a Medical Device

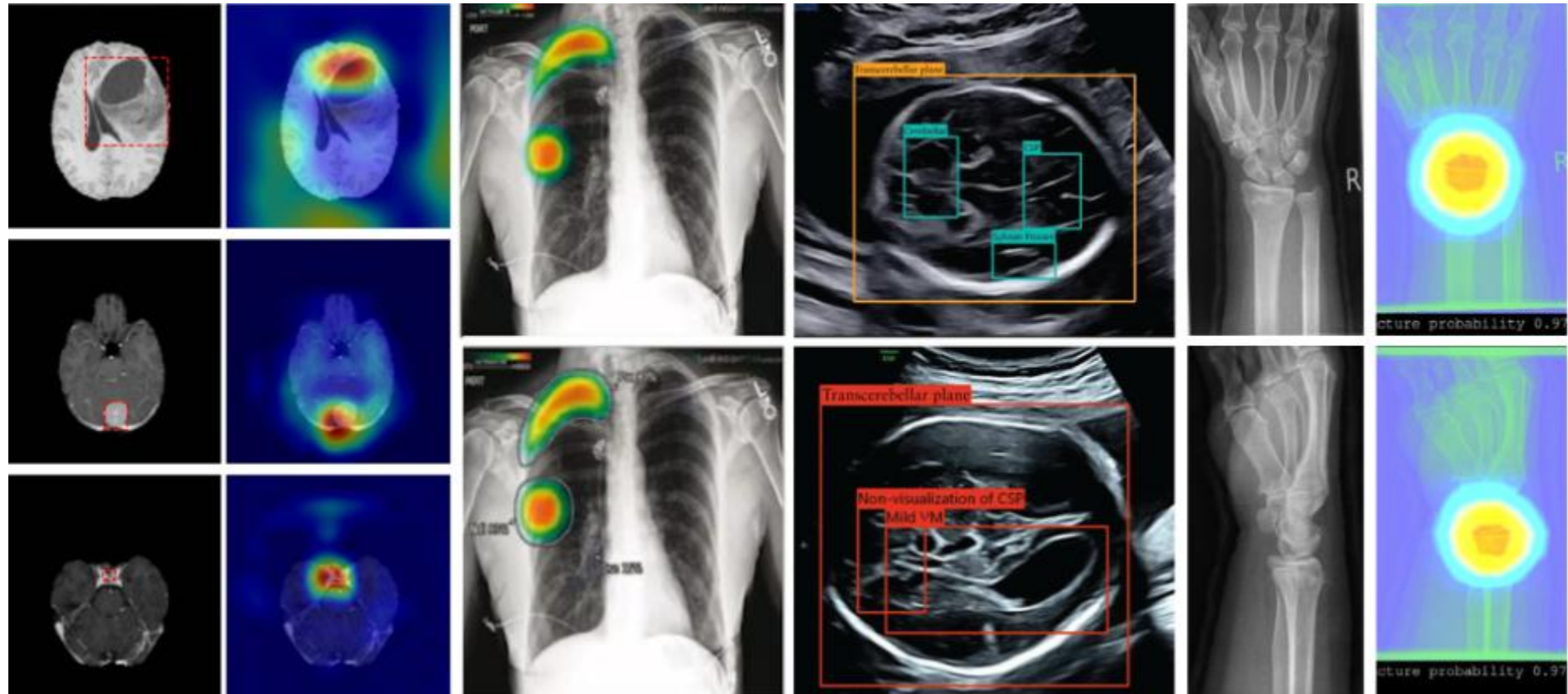
## MATRIZ DE RIESGO IMDRF: DETERMINACIÓN DE LA CATEGORÍA REGULATORIA



# Artificial Intelligence Diagnostic Imaging Platform



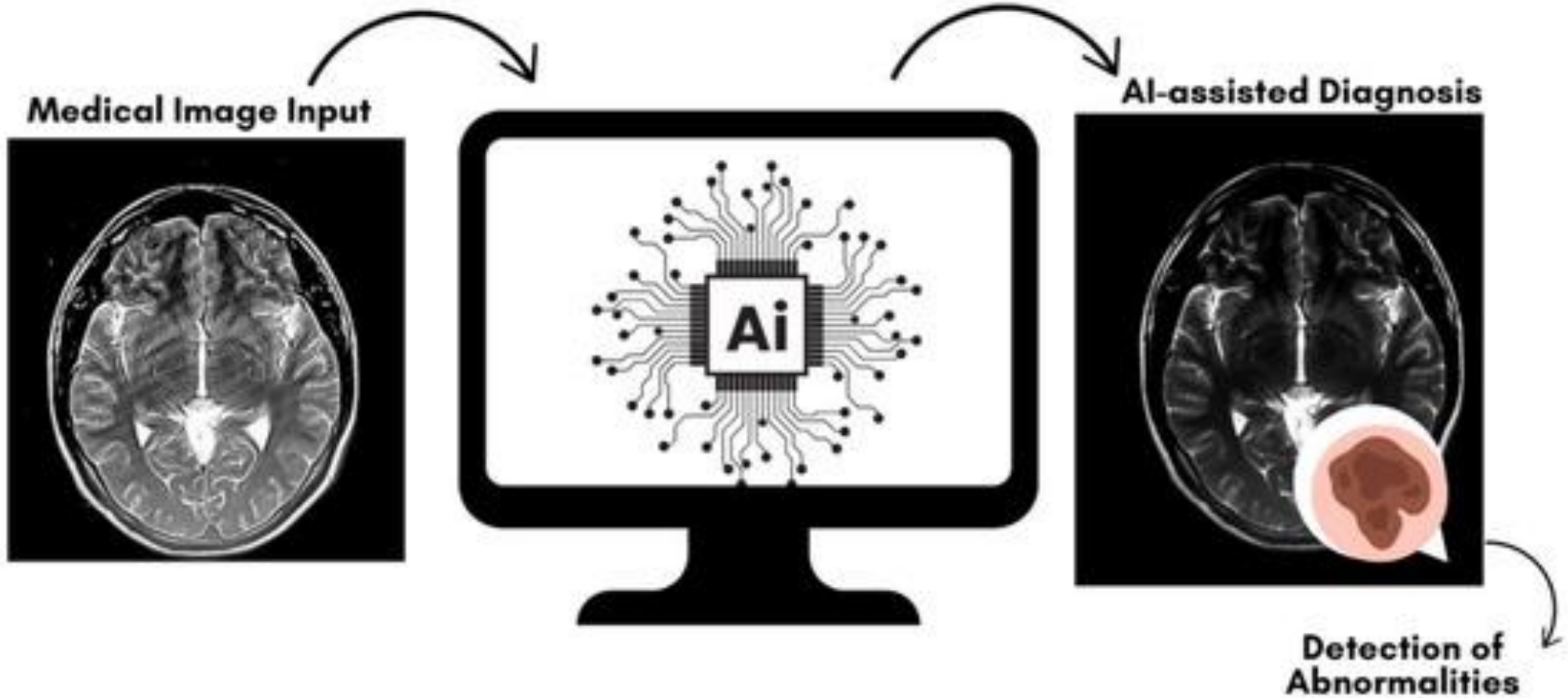
# Artificial Intelligence Diagnostic Imaging Platform



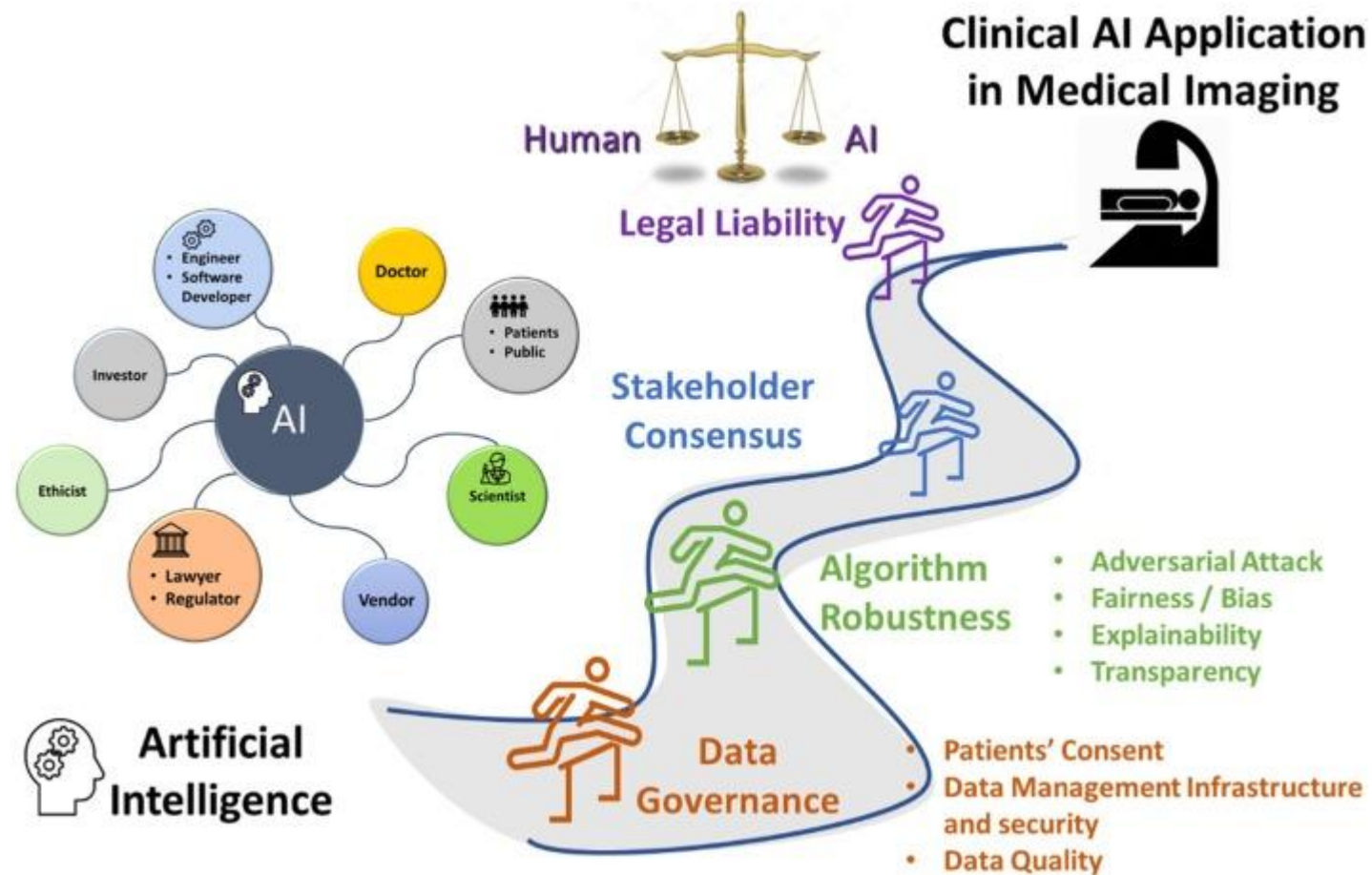
Fonte: [kritikalsolutions.com/artificial-intelligence-in-medical-imaging/](https://kritikalsolutions.com/artificial-intelligence-in-medical-imaging/)



# Artificial Intelligence Diagnostic Imaging Platform



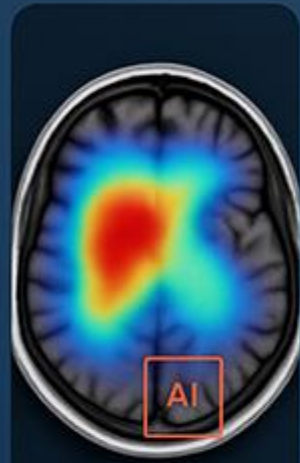
# Artificial Intelligence Diagnostic Imaging Platform



# Artificial Intelligence Diagnostic Imaging Platform

www.kenthospitals.com

## AI-Assisted Imaging



MRI

Original  
MRI



CT



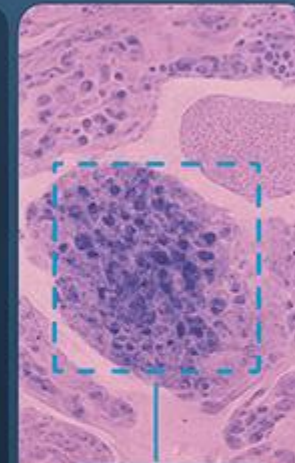
Ultrasound

Alert



PET

Hyper-  
metabolic



Carcinoma

Digital  
Pathology

## Artificial Intelligence Diagnostic Imaging Platform

# AI-Assisted Imaging in Healthcare



**MRI**

Deep Learning  
Reconstruction

**CT**

AI Scan  
Analysis

**PET**

Image  
Enhancement

**AI**

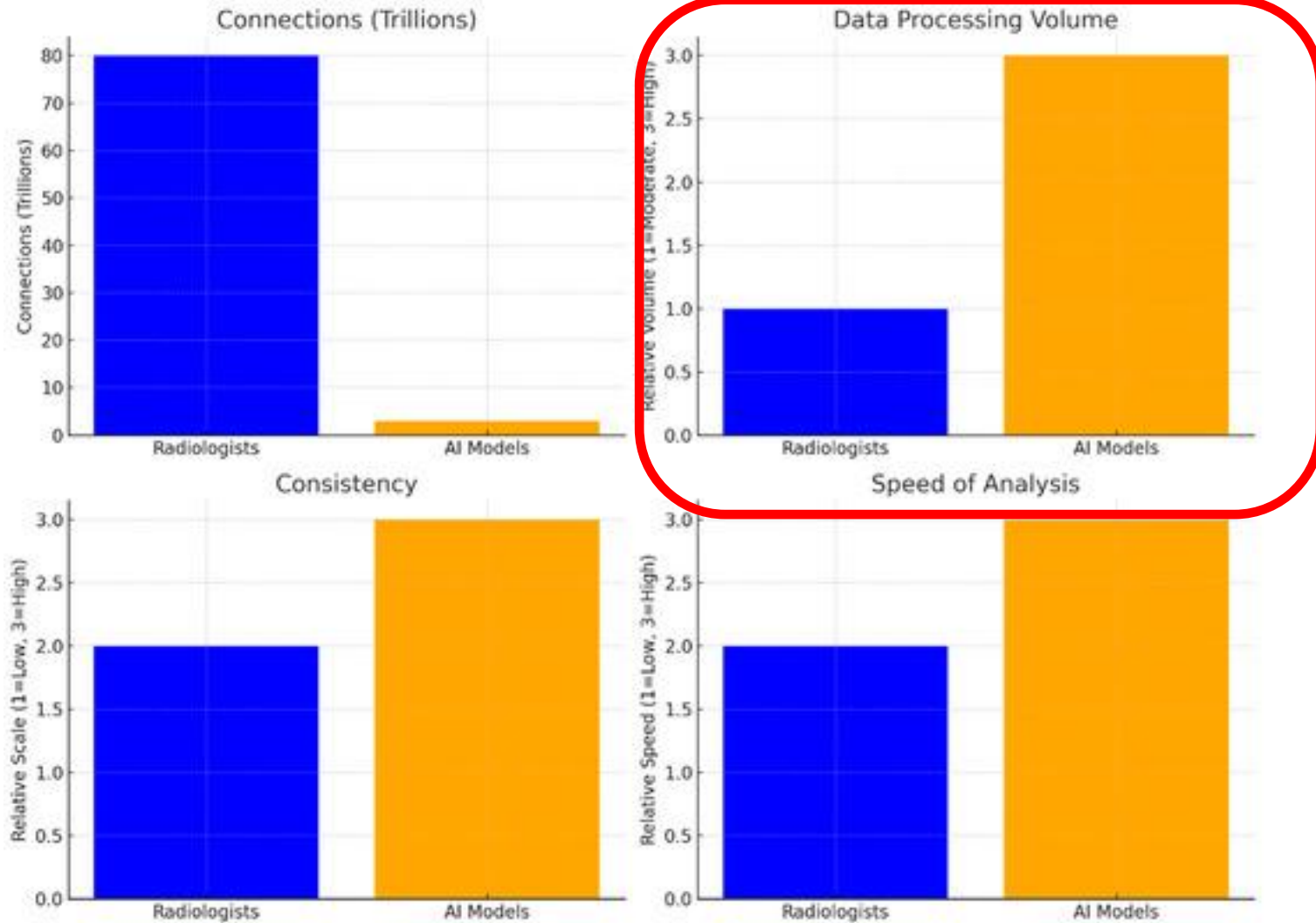
Diagnosis

**Digital  
Pathology**

[www.kenthospitals.com](http://www.kenthospitals.com)



# Artificial Intelligence Diagnostic Imaging Platform



# Software as a Medical Device

BENEFICIOS PARA PACIENTES	BENEFICIOS PARA MÉDICOS E INSTITUCIONES
Diagnósticos más rápidos y precisos	Apoyo en la toma de decisiones clínicas
Monitoreo remoto de salud en tiempo real	Reducción de errores diagnósticos y terapéuticos
Tratamientos personalizados según el perfil genético	Optimización del tiempo en consultas e informes
Acceso facilitado a especialistas mediante telemedicina	Gestión más eficiente de recursos hospitalarios
Prevención de complicaciones en enfermedades crónicas	Apoyo en investigación y descubrimiento de nuevos medicamentos
Mejor experiencia y adherencia al tratamiento	Capacitación avanzada con simuladores de IA



# IA EN LA PRÁCTICA MÉDICA

## Desafíos de Validación

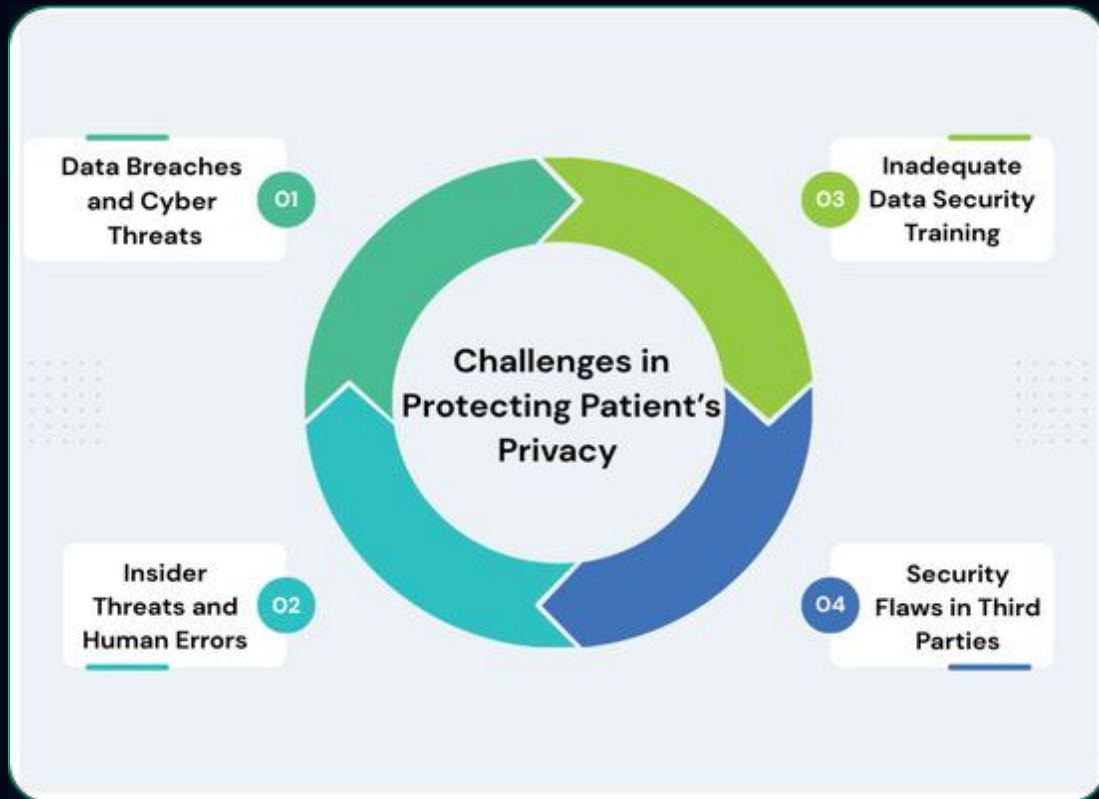
Sistemas de apoyo a la decisión clínica (CDS) son críticos. La legislación exige:

**Validación rigurosa:** Pruebas en poblaciones locales (diversidad brasileña).

**Responsabilidad médica:** La IA es una herramienta, no un sustituto del juicio clínico.  
Auditabilidad de la base de datos de entrenamiento.



# PROTECCIÓN DEL PACIENTE



## Intersección LGPD y PL 2338

Los datos de salud son altamente sensibles. La gobernanza digital debe garantizar:

Anonimización y seudonimización efectiva.

Control estricto de accesos y registros (logs).

Transparencia sobre el uso de datos en investigación.

# GRC no Setor de Saúde

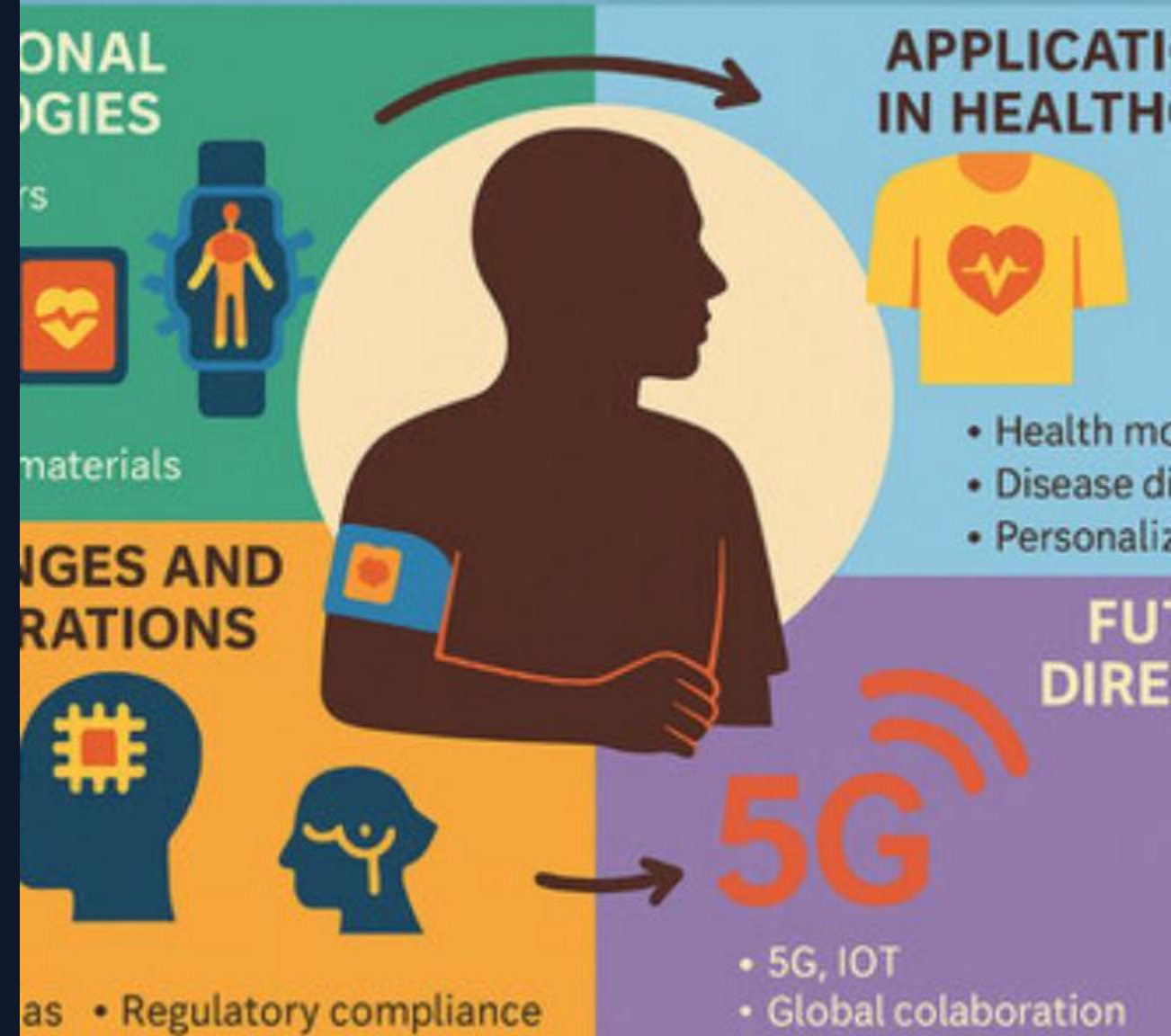
## Diagnósticos e Privacidade

A integração da IA na medicina exige conformidade estrita com a LGPD e as novas diretrizes do PL 2338. Sistemas de diagnóstico assistido e triagem hospitalar são considerados de alto risco devido ao impacto potencial na integridade física.

Validação clínica de algoritmos.

Anonimização em Big Data de saúde.

## DRIVEN WEARABLE BIOELECTRO IN DIGITAL HEALTHCARE



---

# Impacto en el Sector Salud

IA en Diagnósticos, Tratamientos y Datos Clínicos

## **Los hospitales con inteligencia artificial están en el punto de mira de Brasil.**

La Agencia Nacional de Vigilancia Sanitaria (Anvisa) y el Ministerio de Salud están acelerando la regulación de los hospitales inteligentes en el país.

Esta iniciativa surge tras visitas a hospitales en China, donde la inteligencia artificial ya forma parte de la atención rutinaria. El plan incluye:

- la creación de una red nacional de hospitales inteligentes
- una inversión de 300 millones de dólares
- el uso de IA para diagnóstico, monitorización y gestión
- la previsión de la primera unidad pública para 2029



La Agencia Nacional de Vigilancia Sanitaria de Brasil (Anvisa) exige que el software de telemedicina que utiliza Inteligencia Artificial (IA) con fines médicos se registre como Dispositivo Médico (SaMD).

El uso de estos sistemas debe garantizar la seguridad, la transparencia algorítmica y la mitigación de sesgos durante el apoyo a la toma de decisiones clínicas.

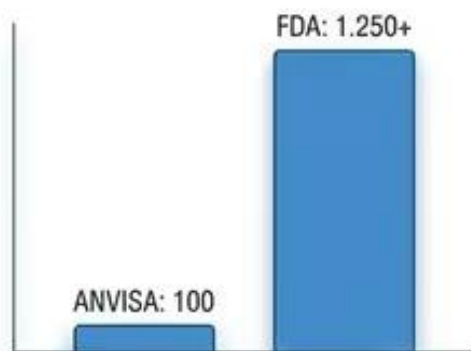
Las normas, responsabilidades y procedimientos de cumplimiento para el uso de estas tecnologías en Brasil incluyen:

**Clasificación y Registro (RDC 657/2022 y RDC 751/2022):** Anvisa clasifica el software médico según el riesgo. Los sistemas de triaje o diagnóstico autónomo requieren un control y una notificación rigurosos.

**Requisitos específicos para la IA:** Si el software utiliza IA para lograr su propósito médico (como informes automatizados o análisis de imágenes), la empresa debe presentar un informe detallado que justifique la técnica de IA utilizada, el tamaño de las bases de datos, el historial de entrenamiento y la validación clínica del algoritmo.

**Responsabilidad compartida:** Si bien la IA actúa como herramienta de apoyo a la toma de decisiones, la Resolución 2454/2026 del CFM establece que la decisión final, el diagnóstico y la responsabilidad civil recaen **exclusivamente en el médico.**





VOLUME DE APROVAÇÕES DE SOFTWARE MÉDICO



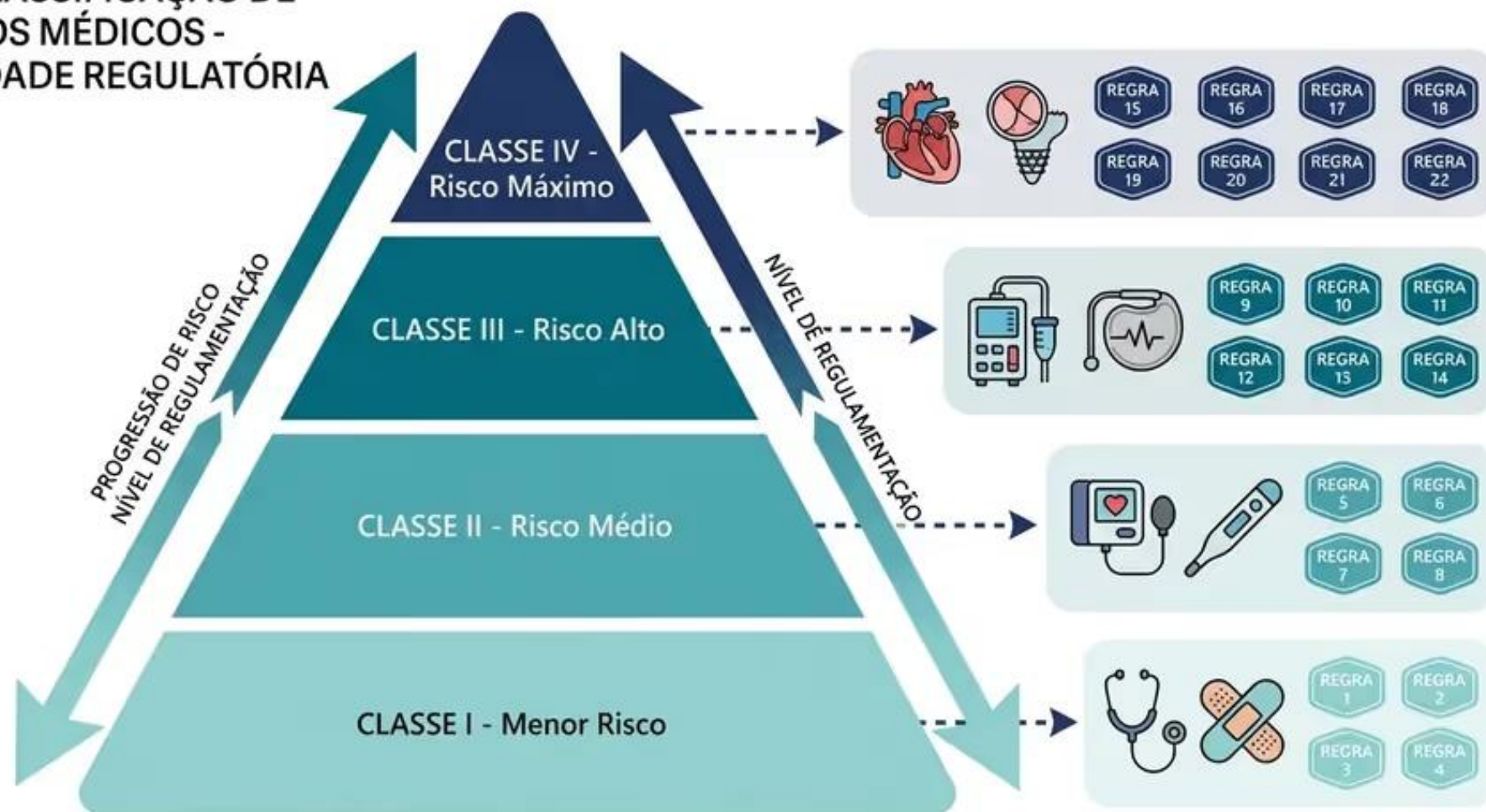
LINHA DO TEMPO REGULATÓRIA

### COMPARATIVO DE SISTEMAS PARA SAMD

ANVISA	FDA	EU MDR/AI ACT
<p>VOLUME DE APROVAÇÕES</p>	<p>VOLUME DE APROVAÇÕES</p>	<p>VOLUME DE APROVAÇÕES</p>
<b>VIAS DISPONÍVEIS</b>		
<p>REGULAR</p>	<p>SIMPLIFICADA</p>	<p>NOTIFICAÇÃO</p>
<b>MARCOS TEMPORAIS RELEVANTES</b>		
<p>NOTIFICAÇÃO</p>	<p>NOTIFICAÇÃO</p>	<p>CERTIFICAÇÃO</p>

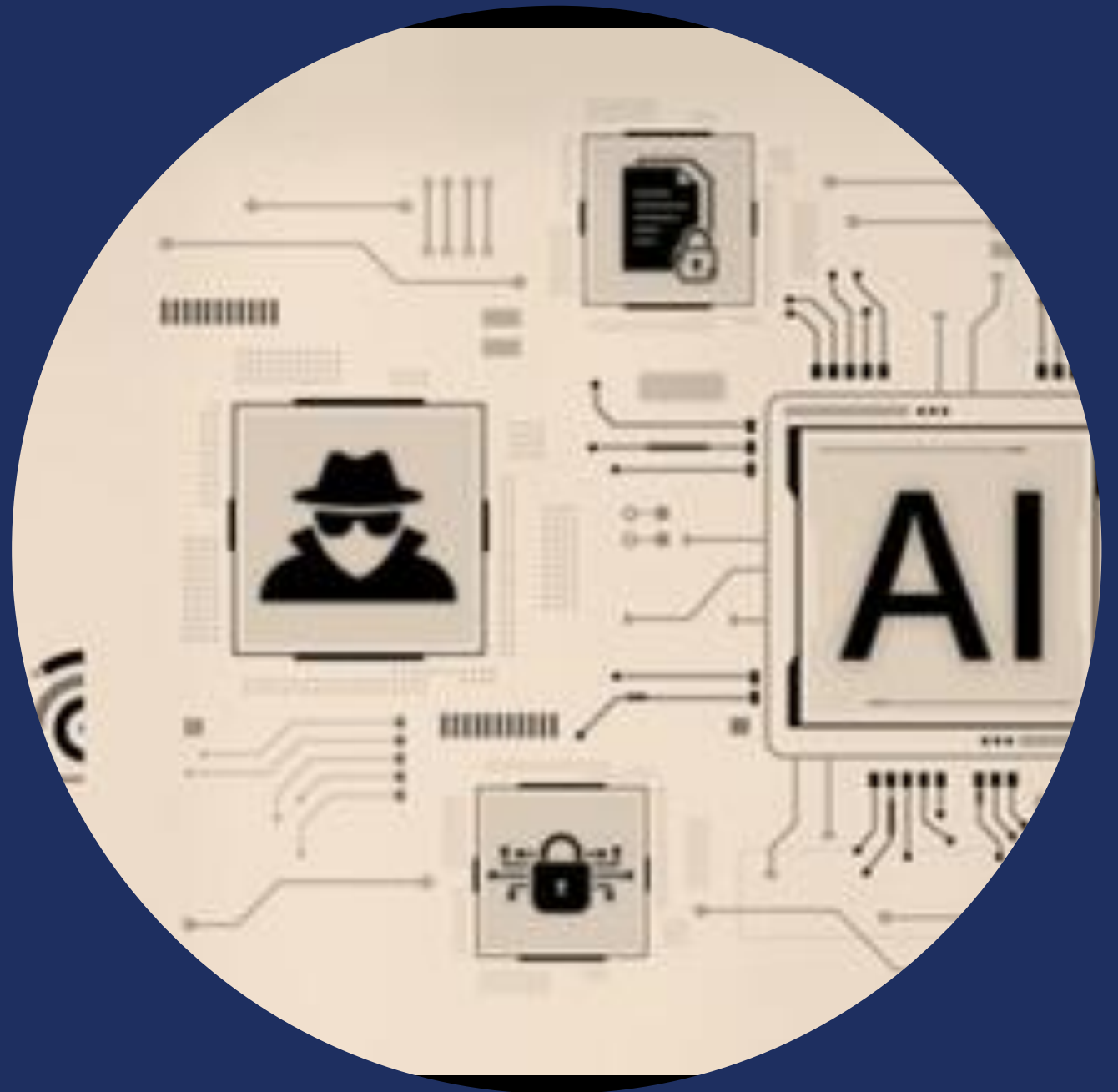
COMPARATIVO DE SISTEMAS PARA SAMD

## FLUXO DE CLASSIFICAÇÃO DE DISPOSITIVOS MÉDICOS - CONFORMIDADE REGULATÓRIA



O artigo apresenta a estrutura de classificação de dispositivos médicos em 4 classes de risco com 22 regras agrupadas por tipo de dispositivo. Uma visualização desta hierarquia facilita a compreensão do sistema regulatório.

# RESUMEM



# HACIA UNA IA ÉTICA

## Resumen Ejecutivo

Brasil está posicionándose como un líder en regulación ética en el Sur Global. El éxito

dependerá del equilibrio entre:

Protección intransigente de derechos humanos.

Fomento de un ecosistema de innovación ágil.

Cooperación internacional en estándares técnicos.

**100%**  
Compromiso Ético



# Software as a Medical Device

## Healthcare AI Risk Management

### Risks in Healthcare AI:

- Bias
- Privacy Breaches
- Lack of Explainability

### Core Principles:

- Transparency
- Fairness
- Human Oversight

### Why It Matters:

- Protect Patients
- Ensure Compliance
- Maintain Trust

### Risk Assessment:

- Model Validation
- Stress Testing
- Performance Monitoring

### Governance & Compliance:

- HIPAA
- GDPR
- FDA guidelines

### Future Outlook:

- Oversight
- Collaboration
- Responsible AI

# Software as a Medical Device

En resumen, Brasil está muy avanzado en las propuestas para aplicar la IA a los ciudadanos y las empresas.

O mercado brasileiro já conta com aproximadamente **500 softwares registrados como SaMD** software adaptável Predetermined Change Control Plan (PCCP) e requisitos de cibersegurança baseados na **IEC 81001-5-1**.



# Critical Success Factors

- Conduct awareness sessions or deliver communications on the benefits of the GRC initiative for Generative AI and Machine Learning;
- Performance measurements must be reported for each business case in Artificial Intelligence solutions, to continue building confidence and trust and enable any corrective actions to be taken on time (KPI and KRI);
- Set of activities and outcomes in a given domain and the collective rollup of trust factor practices;

**Gracias!**

## Adriano Neves

CAIO (Chief Artificial Intelligence Officer)

[www.metaqualys.com](http://www.metaqualys.com)

Executive Advisor

ISACA São Paulo Chapter

[adriano.neves@isaca.org.br](mailto:adriano.neves@isaca.org.br)

+55 11 98131-6246

<https://br.linkedin.com/in/adriano-neves-ph-d-pmp-cgeit-crisc-csm-5161b3>



Adriano Neves, Ph.D, PMP, CPDSE, CGEIT,  
CRISC, CSM  
Director, Digital Trust

