



Pilares de #IA #Observatorio #Guatemala

Guatemala, agosto del 2026

Introducción:

La inteligencia artificial (IA) es clave para Guatemala porque permite modernizar los servicios públicos, impulsar la productividad de los pequeños negocios y reducir las grandes brechas de desarrollo social. El país avanza en esta visión a través de iniciativas como la [Evaluación del Panorama de IA \(AIIA\)](#) impulsada por el gobierno y agencias internacionales. [1, 2, 3, 4]

Oportunidades y Beneficios

- **Gobierno y trámites:** Ayuda a simplificar procesos del Estado y mejorar la atención en salud y educación. [1, 2]
- **Emprendimiento y economía:** Facilita que pequeños negocios y comercios locales automaticen ventas y analicen datos sin requerir grandes recursos. [1]
- **Innovación regional:** Permite al país sumarse a las discusiones globales sobre gobernanza tecnológica para no quedarse atrás frente a mercados avanzados. [1, 2]

Retos Actuales en el País

- **Falta de regulación y ética:** Se necesita una ley de protección de datos para evitar que los algoritmos discriminen a la economía informal o a poblaciones vulnerables.
- **Brecha de talento:** Hay escasez de expertos locales en ciencia de datos, lo que obliga al país a buscar capacitación constante.
- **Dependencia externa:** La falta de infraestructura propia hace que los datos de los ciudadanos se procesen en servidores extranjeros. [1, 2]

Política de IA de Guatemala:

Guatemala no cuenta con una política ni con regulación de inteligencia artificial específica ni con un regulador técnico. El país se encuentra en una fase de co-creación y diagnóstico, articulando su primera Estrategia Nacional de Inteligencia Artificial enfocada principalmente en el sector público. [1, 2]

La política de IA avanza a través de las siguientes acciones institucionales y diagnósticos internacionales:

1. Co-creación de la Estrategia Nacional

La [Comisión Presidencial de Gobierno Abierto y Electrónico \(GAE\)](#) lidera el diseño de la estrategia para el Organismo Ejecutivo. El proceso cuenta con el apoyo técnico del [Programa de las Naciones Unidas para el Desarrollo \(PNUD\)](#) y financiamiento europeo para asegurar un enfoque ético y de servicio público. [1, 2, 3, 4]

2. Evaluaciones Globales de Preparación

- **Modelo AILA:** La medición del [Panorama de la Inteligencia Artificial \(AILA\)](#) sirve como base para construir gobernanza de datos y alianzas con la academia. [1, 2]
- **Metodología RAM:** La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco) entregó recientemente a la **Superintendencia de Telecomunicaciones (SIT)** el informe de *Evaluación de la Preparación para la Ética de la IA*. Este documento funciona como hoja de ruta para mitigar riesgos éticos y exclusión social. [1, 2]

3. Vacíos Legales Críticos

La regulación integral en el sector privado sigue estancada debido a que **Guatemala carece de una ley general de protección de datos personales**. Organizaciones civiles como [Diálogos](#) proponen un avance por fases que empiece

por prohibir decisiones automatizadas sin supervisión humana en áreas críticas como solicitudes de asistencia social, créditos bancarios y justicia penal. [, 2]

Pilares propuestos por Observatorio:

El observatorio de tecnología de Guatemala ha desarrollado un plan básico del tema de IA debido a la falta del tema de la política. Este se publicó en el 2024 y puede ser accedido en: <https://observatorioca.tech/estrategia-nacional-de-guatemala-de-inteligencia-artificial/>

En función es esta estrategia y al alto numero de proyectos que se estan ya desarrollando en el país con inteligencia artificial, se propuso tener 5 pilares de apoyo por parte del observatorio:

- Certificaciones para IA
- Competencias de IA
- Ciberseguridad e IA
- Avance en políticas de IA
- Indicadores de impacto de IA

Certificaciones para IA:

Las certificaciones en Inteligencia Artificial (IA) y Ciberseguridad son actualmente pilares estratégicos para profesionales y empresas, ya que validan habilidades técnicas en un mercado con escasez de talento especializado. La importancia se basa en:

- Validación y Confianza: Certifican que el profesional ha superado estándares rigurosos de organismos competentes, diferenciándolo en procesos de selección.
- Aumento Salarial: Certificaciones como CompTIA Security+ o Certified Ethical Hacker (CEH) pueden elevar el promedio salarial anual por encima de los \$67,000 USD.
- Especialización en IA: Permiten dominar herramientas de aprendizaje profundo y modelos de lenguaje, habilidades que los empleadores valoran para la toma de decisiones informada.
- Actualización Continua: En ciberseguridad, certificaciones como la CEH v13 ya integran módulos de defensa basados en IA para enfrentar amenazas modernas.
- Cumplimiento y Ética: Normas como la ISO/IEC 42001 ayudan a gestionar riesgos éticos y de privacidad en sistemas de IA, promoviendo transparencia.

- Protección de Activos: Profesionales certificados aseguran la continuidad del negocio al proteger la propiedad intelectual y evitar pérdidas financieras por ciberataques.
- Ventaja Competitiva: Contar con personal certificado mejora la reputación de la marca y facilita el acceso a nuevos mercados internacionales.

Las certificaciones recomendadas al 2026 son:

- Ciberseguridad: CISSP, Security+, CEH v13 para protección de datos, hacking ético con IA y gestión de riesgos.
- IA: ISO/IEC 42001, AWS Certified AI para gestión ética, gobernanza de datos y despliegue de modelos.
- Híbrido: Microsoft Azure Security Engineers para seguridad en la nube impulsada por automatización de IA.

Las certificaciones de ISO sugeridas para IA en general son:

- ISO/IEC 23894:2023 - Guidance on Risk Management for AI
- ISO/IEC TR 24028:2020 - Overview of Trustworthiness in Artificial Intelligence
- ISO/IEC TR 24027:2021 - Bias in AI Systems and AI-Aided Decision Making
- ISO/IEC 42001:2023 - Artificial Intelligence Management System (AIMS)
- ISO/IEC 23053:2022 - Framework for AI Systems Using Machine Learning
- ISO/IEC 22989:2022 - Artificial Intelligence — Concepts and Terminology
- ISO/IEC 5338 - AI Lifecycle Management
- ISO/IEC 31700 - Privacy by Design in AI

Los cursos de certificaciones de IA se llevan a cabo regularmente en el Observatorio. Interesados: info@mzaghi.com

Competencias para IA:

Según la Organización Internacional del Trabajo (OIT), frente al avance de la tecnología, los empleadores demandan sobre todo competencias cognitivas, socioemocionales y técnicas generales en lugar de conocimientos hiperespecializados en programación de sistemas. El principal desafío no es que todos aprendan a crear algoritmos, sino capacitar a la fuerza laboral para trabajar de forma eficaz junto a las máquinas. [1, 2]

Competencias Clave Destacadas por la OIT

- **Pensamiento crítico:** Para evaluar con criterio y adaptar de forma segura los contenidos generados por la tecnología.
- **Competencias socioemocionales:** Como la comunicación, la resiliencia y el trabajo en equipo, que los sistemas automatizados no pueden imitar.
- **Resolución de problemas:** Para conectar ideas complejas y utilizar las herramientas digitales como un apoyo operativo.
- **Aprendizaje permanente:** La capacidad de actualizar los conocimientos a lo largo de toda la vida laboral ante los cambios del mercado.

La Organización Internacional del Trabajo (OIT) sostiene que el verdadero desafío en la era de la inteligencia artificial **no consiste en que toda la fuerza de trabajo aprenda a desarrollar IA, sino en potenciar las "competencias fundamentales" para trabajar junto a ella.** [1, 2]

Según el informe global de la OIT sobre aprendizaje permanente y habilidades, las ofertas de empleo demuestran que las empresas buscan perfiles integrales. Los empleadores valoran la combinación de conocimientos técnicos específicos con sólidas capacidades humanas y cognitivas. [1, 2]

El marco de competencias que promueve la [OIT](#) frente a la disrupción de la IA se agrupa en cuatro pilares esenciales: [1, 2]

1. Competencias Socioemocionales (Habilidades Blandas)

Permiten una interacción efectiva en entornos donde la IA automatiza las tareas rutinarias. [1, 2]

- **Comunicación efectiva:** Capacidad para transmitir ideas con claridad y negociar.
- **Trabajo en equipo y colaboración:** Coordinación en equipos multidisciplinares e interactivos.
- **Inteligencia emocional:** Gestión de relaciones, empatía y resolución de conflictos en entornos cambiantes. [1, 2, 3, 4, 5]

2. Competencias Cognitivas y Metacognitivas

Son las facultades humanas intelectuales complejas que la IA no puede replicar ni sustituir. [1]

- **Pensamiento crítico:** Evaluación de los sesgos, errores y resultados generados por los modelos de IA.

- **Resolución de problemas complejos:** Capacidad de planificar, organizar y estructurar soluciones ante nuevos desafíos.
- **Creatividad e innovación:** Generación de ideas disruptivas combinando el criterio humano con el soporte tecnológico.
- **Aprendizaje permanente (Lifelong learning):** Capacidad de autorreflexión y "aprender a aprender" para adaptarse a la evolución de las herramientas digitales. [1, 2, 3, 4, 5, 6]

3. Competencias Digitales Básicas y de Datos

Garantizan una alfabetización tecnológica óptima para adoptar los nuevos sistemas de gestión digital. [1, 2]

- **Alfabetización en información y datos:** Localizar, evaluar y organizar datos masivos (Big Data), identificando fuentes confiables.
- **Interacción con sistemas de IA:** Saber comunicarse con la IA (como redactar un *prompt* o instrucción adecuada) e integrar sus aplicaciones en los flujos diarios de trabajo.
- **Ciberseguridad:** Operar de manera segura en entornos virtuales protegiendo los datos personales e institucionales. [1, 2, 3, 4]

4. Especialidades Técnicas y Éticas (Para perfiles específicos)

Habilidades requeridas en menor proporción en el mercado general, pero vitales para la gobernanza del área. [1, 2]

- **Ciencia de datos y aprendizaje automático:** Desarrollo y optimización técnica de los algoritmos de IA.
- **Ética de la IA:** Comprensión del impacto social, sesgos algorítmicos, privacidad de datos y mitigación de desigualdades en el entorno laboral. [1, 2, 3]

Los cursos de competencias de IA se llevan a cabo regularmente en el Observatorio. Interesados: info@mzaghi.com

Ciberseguridad e IA:

La relación entre la Inteligencia Artificial (IA) y la ciberseguridad es una carrera armamentista tecnológica de doble filo. Por un lado, funciona como una defensa automatizada ultrarrápida para proteger sistemas, pero por el otro, proporciona a

los ciberdelincuentes herramientas sofisticadas para evadir la seguridad tradicional.

Esta interacción se divide en tres ejes fundamentales:

La IA como Escudo (Defensa)

Las organizaciones emplean herramientas defensivas de IA para ir un paso adelante de las amenazas y mitigar incidentes.

- Detección de anomalías: Monitorea patrones de comportamiento en redes para hallar amenazas que los humanos no ven.
- Respuesta automatizada: Aísla sistemas comprometidos y bloquea direcciones IP maliciosas de forma inmediata.
- Filtro de alertas: Reduce la fatiga de los analistas al clasificar miles de alertas en minutos.

Auditoría de código: Analiza millones de líneas de software de manera autónoma para corregir vulnerabilidades históricas.

La IA como Arma (Ataque)

Los atacantes se aprovechan de los modelos avanzados de IA para automatizar e intensificar sus ofensivas globales.

- Phishing remasterizado: Creación de correos e historias de fraude hiperpersonalizadas y sin errores gramaticales.
- Deepfakes: Suplantación de voz y video en tiempo real para engañar a empleados y saltarse controles biométricos.
- Malware mutante: Desarrollo de software malicioso que altera su propio código para evitar ser detectado por antivirus clásicos.
- Descubrimiento de fallas: Uso de modelos de lenguaje para encontrar debilidades críticas en infraestructuras corporativas en segundos.

Seguridad de la propia IA (Protección del Modelo)

Una nueva rama de la ciberseguridad se enfoca en resguardar los propios sistemas, datos y agentes de IA corporativos.

- Ataques de envenenamiento: Evita que atacantes alteren los datos de entrenamiento para manipular las decisiones de la IA.
- Inyección de 'prompts': Protege los modelos lingüísticos contra instrucciones maliciosas diseñadas para filtrar datos confidenciales.

- **Control de agentes autónomos:** Supervisa las acciones de agentes automatizados para evitar que tomen decisiones perjudiciales en la red

En resumen, la relación entre la inteligencia artificial (IA) y la ciberseguridad es profunda y de doble vía, destacándose en tres ejes: **defensa proactiva, amenazas automatizadas y vulnerabilidad de los propios sistemas de IA**. La IA sirve como un escudo inteligente para bloquear fraudes, pero también como un arma sofisticada para los atacantes. [1, 2]

Defensa y Protección

- **Detección rápida:** Analiza millones de datos en tiempo real para hallar virus y estafas de tipo phishing antes de que dañen una red.
- **Respuesta automática:** Bloquea accesos extraños o ataques de manera inmediata sin requerir personal humano constante.
- **Menos errores:** Disminuye las falsas alertas y ayuda a predecir fallas futuras en los equipos. [1, 2, 3, 4]

Nuevos Riesgos y Ataques

- **Ataques mejorados:** Los criminales usan la IA para crear mensajes de engaño más reales y automatizar códigos maliciosos.
- **Perfiles falsos:** Se crean identidades en línea idénticas a las reales para robar datos o estafar personas.
- **Fraude en voz y texto:** Se imitan patrones humanos para burlar filtros de seguridad. [1, 2, 3, 4]

La IA como Blanco

- **Sistemas frágiles:** Los programas de IA también pueden ser hackeados o engañados mediante la manipulación de datos.
- **Privacidad:** El uso de datos sensibles para entrenar modelos de IA expone información si no se maneja de forma segura

Si quieres recibir un curso básico de Ciberseguridad e IA, favor contactar a info@mzaghi.com

Políticas nacionales e institucionales de IA:

La diferencia principal radica en el alcance y el nivel de aplicación: la **política nacional de IA** es una estrategia macro del Estado para todo el país, mientras que las **políticas institucionales de IA** son normas internas de una organización o empresa específica. [1, 2, 3]

Política Nacional de Inteligencia Artificial

- **Alcance:** Aplica a todo el territorio nacional, abarcando al sector público, privado, educativo y a la sociedad.
- **Objetivo:** Fomentar la innovación tecnológica, el desarrollo económico, la seguridad jurídica y la protección de los derechos de los ciudadanos.
- **Responsable:** El gobierno central a través de ministerios u órganos rectores estatales. [1, 2, 3, 4, 5]

Políticas Institucionales de Inteligencia Artificial

- **Alcance:** Limitado exclusivamente a los empleados, procesos y sistemas de una organización o institución (como una empresa, universidad o ministerio particular). [1, 2]
- **Objetivo:** Regular el uso ético, seguro y práctico de las herramientas de IA en el trabajo diario, protegiendo los datos propios y evitando riesgos legales. [1, 2]
- **Responsable:** La administración, directiva o comité de ética de cada organización. [1, 2]

El estatus de la política nacional de IA se ha comentado en la introducción, pero faltaría definir que es una política institucional:

Una política institucional de Inteligencia Artificial es un conjunto de normas, directrices y reglas internas que regulan cómo una organización específica utiliza, desarrolla o implementa tecnologías de IA.

Características clave

- **Propósito:** Proteger la seguridad de la empresa, mitigar riesgos legales y asegurar un uso ético de la tecnología.
- **Aplicación:** Es de cumplimiento obligatorio únicamente para los empleados, colaboradores y proveedores de esa institución.

- **Personalización:** Se adapta a las necesidades, valores y objetivos comerciales de la organización.

Componentes comunes de esta política

- **Uso permitido y prohibido:** Define qué herramientas de IA (como ChatGPT) se pueden usar y para qué tareas específicas.
- **Privacidad y confidencialidad:** Prohíbe introducir datos sensibles de la empresa o de clientes en plataformas de IA públicas.
- **Supervisión humana:** Exige que un empleado revise y valide siempre cualquier resultado generado por una IA antes de usarlo.
- **Transparencia:** Obliga a notificar a los clientes o usuarios cuando se esté utilizando IA para interactuar con ellos o procesar su información.
- **Propiedad intelectual:** Clarifica a quién pertenecen los contenidos o códigos creados con ayuda de herramientas automatizadas

Indicadores de impacto de IA:

Los indicadores de impacto de IA son **métricas y valores numéricos** que sirven para saber **qué tanto valor real, cambio o beneficio** generan los sistemas de inteligencia artificial en una empresa, un proceso o la sociedad. [1, 2, 3, 4]

A diferencia de las pruebas técnicas que miden si el programa funciona bien por dentro (como la precisión del código), estos indicadores miden el resultado final afuera. [1]

Tipos de Indicadores de Impacto

- **Impacto Económico**
 - **Retorno de inversión (ROI):** compara el dinero ganado frente al costo de usar la IA.
 - **Reducción de costos:** mide cuánto dinero se ahorra al automatizar tareas. [1]
- **Impacto Operativo**
 - **Aumento de productividad:** calcula cuánto más rápido o mejor trabajan las personas con ayuda de la IA.
 - **Tiempo de respuesta:** mide la reducción de horas o minutos en atender procesos o clientes. [1]

- **Impacto Social y Humano**

- Adopción real: cuenta cuántas personas usan la herramienta en su día a día.
- Satisfacción del usuario: evalúa si las personas se sienten más ayudadas o contentas con el resultado

Si existen metodologías y marcos estructurados creados por consultoras globales, empresas tecnológicas y organismos internacionales para implementar estos indicadores. [1, 2, 3]

Las metodologías más utilizadas se dividen según su enfoque:

1. El Marco de las 5 Capas (McKinsey)

Esta metodología ayuda a conectar el funcionamiento técnico de la IA directamente con el dinero que gana la empresa, creando una línea auditable. Se mide de abajo hacia arriba: [1]

- **Capa 1: Rendimiento Técnico:** ¿El modelo de IA responde rápido y sin errores?
- **Capa 2: Adopción y Uso:** ¿Los empleados usan la herramienta diariamente o la ignoran?
- **Capa 3: KPIs Operativos:** ¿Se redujeron los tiempos de los procesos o los cuellos de botella?
- **Capa 4: Resultados Estratégicos:** ¿Mejoró la satisfacción del cliente o la retención de usuarios?
- **Capa 5: Impacto Financiero:** ¿Cuánto dinero extra generó o cuánto ahorro real de costos logramos? [1, 3]

2. Marco DX (Utilización, Impacto y Costo)

Es la metodología estándar para medir la IA cuando se implementa en equipos de desarrollo de software o ingeniería: [1, 2]

- **Utilización:** Monitorea la telemetría interna (APIs, inicios de sesión, tasa de aceptación de sugerencias de la IA).
- **Impacto directo e indirecto:** Mide las Horas Equivalentes Humanas (HEH) ahorradas combinadas con encuestas de satisfacción del empleado.
- **Costo:** Cruza los datos anteriores con el gasto en tokens y licencias para ver si el costo operativo vale la pena. [, 2, 3, 4]

3. Marco de Evaluación de Impacto de IA (AIA)

Utilizado para proyectos con impacto social, ético o de políticas públicas (promovido por organismos como la OECD). No mide dinero, mide riesgos y capacidades humanas: [1, 2, 3]

- **Nivel de Competencia:** Mide en una escala del 1 al 5 si la IA complementa o sustituye la habilidad humana en tareas complejas.
- **Mitigación de Sesgos:** Indicadores cualitativos y cuantitativos que aseguran que la IA no discrimine en sus decisiones. [1, 2]

Pasos Comunes para Implementar Cualquier Metodología

1. **Establecer la Línea de Base:** Medir cómo funciona el proceso hoy (sin IA) en tiempo, costo y errores. [, 2, 3, 4]
2. **Hacer Despliegue Escalonado (Pruebas A/B):** Entregar la IA solo a un grupo piloto y comparar su impacto contra el grupo que trabaja de forma tradicional. [, 2]
3. **Triangular Datos:** No confiar solo en las métricas automáticas del software. Combinar telemetría con encuestas periódicas de los usuarios para evitar datos falsos.

Si quieres recibir un curso básico de Ciberseguridad e IA, favor contactar a info@mzaghi.com

Que es el Observatorio de Tecnología:

- Que es el observatorio de tecnología: Es una plataforma de apoyo a la transferencia de tecnología, la innovación y el emprendimiento desde la vigilancia tecnológica
- Qué entendemos por observatorio de tecnología: Un observatorio de tecnología es una plataforma de apoyo a la transferencia de tecnología, la innovación y el emprendimiento desde la vigilancia tecnológica
- Qué entendemos por vigilancia tecnológica: Vigilancia tecnológica: Identificación, evaluación y uso de señales débiles para reconocer y advertir en una fase temprana, tecnologías emergentes, discontinuidades tecnológicas (innovaciones disruptivas o rupturistas), oportunidades y amenazas.
- Qué entendemos por tecnología: La tecnología es el conjunto de saberes, conocimientos, experiencias, habilidades y técnicas a través de las cuales

nosotros los seres humanos cambiamos, transformamos y utilizamos nuestro entorno con el objetivo de crear herramientas, máquinas, productos y servicios que satisfagan nuestras necesidades y deseos.

- Para cualquier consulta o comentario adicional, le invitamos a visitar los foros del Observatorio de Tecnología de Guatemala: <https://observatorioca.tech/> o escribir a info@mzaghi.com

Los cursos básicos de como implementar un proyecto de IA de una organización, se llevan a cabo regularmente en el Observatorio. Interesados: info@mzaghi.com