AmCham Panama

Código de Uso Ético de la Inteligencia Artificial

DELL Technologies | Microsoft

Octubre 2025

Créditos y Colaboradores

Agradecimientos Especiales

Este documento ha sido posible gracias a la colaboración de líderes empresariales de diversos sectores de Panamá, expertos internacionales en ética digital, representantes del gobierno nacional y académicos de instituciones educativas panameñas. Agradecemos especialmente a Dell Technologies, Microsoft, GBM, Tigo y Secretaría Nacional de Ciencia, Tecnología e Innovación (SENACYT) por su valiosa colaboración en la construcción de esta guía. Asimismo, extendemos nuestro agradecimiento a Georgia Tech Panama, Cedeño y Méndez, Icaza, González-Ruiz & Alemán, Lombardi Aguilar Group, Sinergía, la Universidad Tecnológica de Panamá (UTP), la Ciudad del Saber y el Instituto Panamericano de Derecho y Tecnología (IPANDETEC) por el suministro de datos clave que enriquecieron este trabajo.

- Cedeño y Méndez - Paula Alzate
- Ciudad del Saber - Jonathan Diaz
- Dell Technologies - Ana Teresa Ferrer, Angel Medina, Anthony Payne, Faustino Aguilar, Jidi Luo, Natalia Montemayor, Niurka Montero
- GBM - Gustavo Cuervo
- Georgia Tech Panamá - Jorge Barnett
- Icaza, González-Ruiz & Alemán - Mariela de la Guardia
- Lombardi Aguilar Group - Álvaro Aguilar
- Microsoft - Edwin Campos
- Secretaria Nacional de Ciencia, Tecnología e Innovación - Eduardo Ortega-Barría
- Sinergia - Dacil Acevedo
- Tigo Panamá - Juan de Dios
- Universidad Tecnológica de Panamá - Martín Candanedo

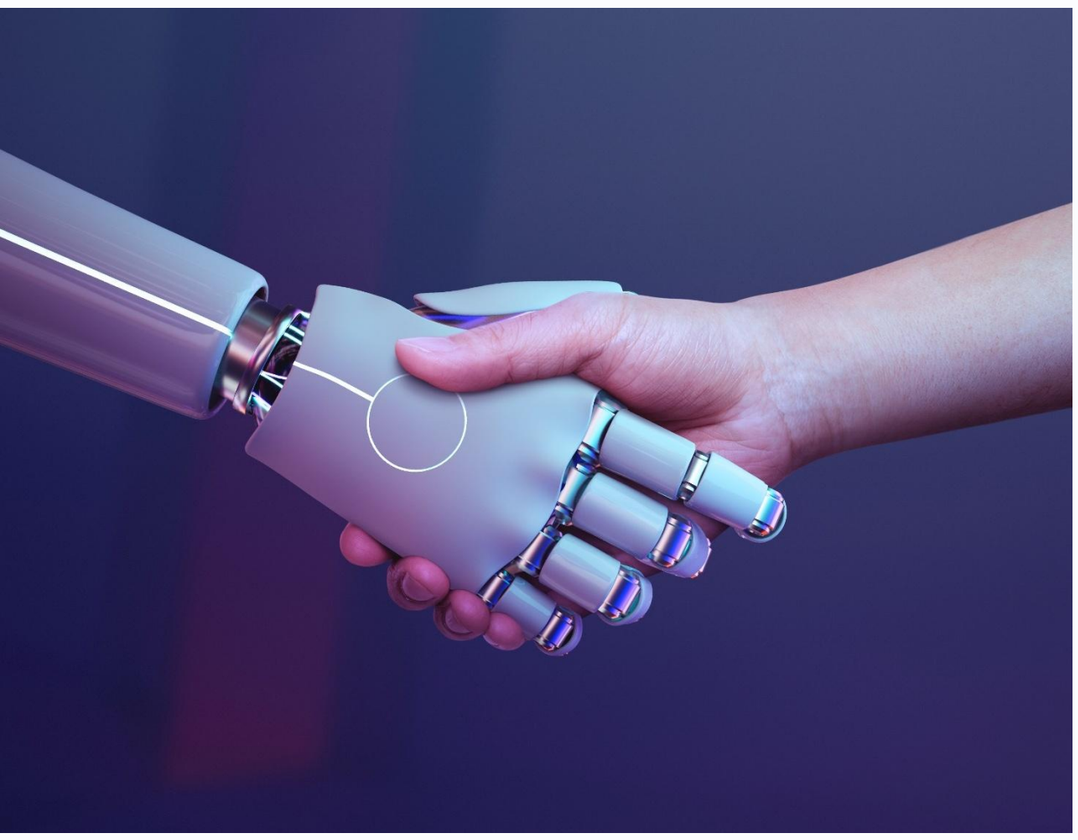
Versión y Actualización

Primera edición, Octubre 2025. Este documento será revisado y actualizado anualmente para reflejar los avances tecnológicos y cambios en el marco regulatorio. La versión digital más reciente está disponible en el sitio web de AmCham Panamá.

Índice

1.1 Introducción

Propósito de la Guía



> *“La tecnología responsable no consiste sólo en ser conscientes de lo que podría ocurrir como resultado de nuestras acciones bien intencionadas. Se trata de estar plenamente comprometidos con el ahora, reevaluando constantemente a quién y qué protegemos y cómo lo hacemos; nunca hemos terminado.”*
>
> — Rebecca Parsons, CTO, Emerita, Thoughtworks

Este documento complementa el **Código de Ética de AmCham Panamá**, estableciendo un marco específico para la implementación responsable de la Inteligencia Artificial (IA) en el entorno empresarial. En un contexto de transformación tecnológica acelerada, es clave contar con principios éticos que orienten su uso, maximizando beneficios y reduciendo riesgos.

La ética de la IA aborda los dilemas morales en la interacción entre tecnología, seres humanos y sociedad. No existe una definición única pero está inspirada en la visión aristotélica de la ética como base de relaciones humanas ideales, esta disciplina busca promover una interrelación justo, transparente y consciente entre humanos y tecnología.*

En Panamá, entidades públicas y privadas ya exploran la IA en sectores como finanzas, logística y salud, lo que refuerza la necesidad de un marco ético. Esta guía ofrece a las empresas miembro de AmCham Panamá una guía práctica para integrar la IA de forma ética, alineada con los valores de responsabilidad, equidad y transparencia que promovemos.

Objetivo principal: Establecer un marco de referencia que permita a las empresas miembro de AmCham Panamá promover el uso ético, responsable y confiable de la inteligencia artificial en el sector empresarial. Este marco busca asegurar que la implementación esté alineada con el principio fundamental de la UNESCO, centrado en el desarrollo y uso de tecnologías que respeten los derechos humanos, la dignidad, la inclusión y la sostenibilidad para fortalecer la confianza del ecosistema empresarial y social.

Objetivos Específicos

Promover una Cultura de Ética Digital y Gobernanza Responsable

Promover el diálogo ético en todos los niveles y estableciendo mecanismos internos para prevenir riesgos y garantizar el uso justo de la IA.

Impulsar la Transparencia, Sostenibilidad y Cooperación Multisectorial

Ofrecer marcos de referencia, asegurando que las soluciones de IA sean explicables y auditables, integrando principios ambientales y promoviendo proyectos con impacto social.

Desarrollar Capacidades y Competitividad Responsable

Desarrollar programas de formación en ética de IA, proporcionar herramientas prácticas para su implementación, y apoyo a las empresas en la adopción de buenas prácticas.

*Fuente: Guía Ética USAID

Capacitación para la Adopción de IA

El Factor Humano: Pilar de la Ética en la IA

La implementación ética de la inteligencia artificial depende principalmente de las personas que la diseñan, desarrollan y utilizan, más que de los algoritmos o políticas escritas. Para traducir los principios éticos en prácticas concretas, es fundamental cultivar una cultura organizacional que valore la ética en la innovación tecnológica. Esto requiere involucrar a todos los niveles—desde la alta dirección hasta los equipos operativos— y asegurar que cuenten con la capacitación y herramientas necesarias para tomar decisiones informadas y responsables.

Programa Integral de Capacitación

Sensibilización General

Sesiones introductorias para toda la organización que expliquen conceptos básicos de IA, potenciales impactos éticos y la responsabilidad compartida en su implementación responsable.

Capacitación Técnica Especializada

Formación profunda para equipos de desarrollo y datos sobre técnicas específicas para mitigar sesgos, mejorar transparencia, implementar privacidad por diseño y evaluar impactos éticos.

Formación para Liderazgo

Programas dirigidos a la alta dirección y mandos intermedios sobre gobernanza de IA, gestión de riesgos éticos, implicaciones estratégicas y creación de culturas organizacionales que prioricen la responsabilidad algorítmica.

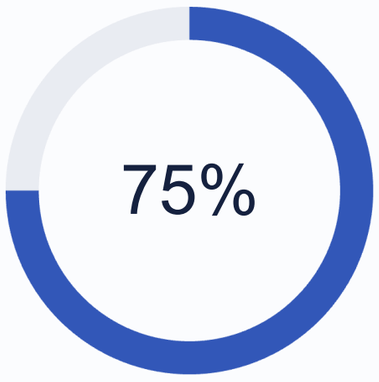
Educación para Usuarios Finales

Recursos accesibles para empleados que utilizan herramientas de IA en su trabajo diario, enfocados en desarrollar pensamiento crítico, reconocer limitaciones de los sistemas y mantener supervisión humana adecuada.

Integración en la Cultura Organizacional

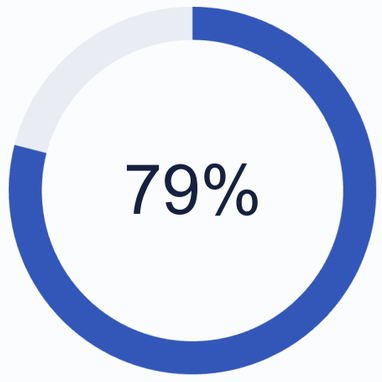
Formación Continua y Especializada

El campo de la ética en IA evoluciona rápidamente, con nuevos desafíos, técnicas y estándares emergiendo constantemente. La capacitación debe concebirse como un proceso continuo, no como un evento único, con actualizaciones regulares y oportunidades para profundizar en áreas específicas.



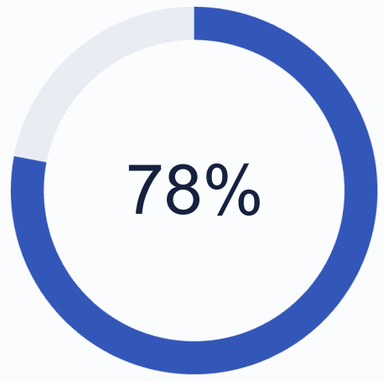
Mejora en eficiencia

Directivos que confirman que la IA optimiza la eficiencia y metodologías de trabajo en sus equipos.



Aumento de moral

Empresas que reportan mejoras significativas en la satisfacción y motivación de sus colaboradores tras implementar herramientas de IA.



Colaboración

Organizaciones donde la IA ha potenciado las dinámicas colaborativas entre empleados.

Fuente: Boston Consulting Group & MIT Sloan Management Review

Integración en la Cultura Organizacional

La integración de la inteligencia artificial (IA) en las empresas debe ir más allá de la simple adopción tecnológica; requiere una alineación profunda con principios éticos que formen parte de la cultura organizacional. Esta responsabilidad no recae únicamente en los equipos técnicos, sino que debe ser compartida por la dirección general, el área de recursos humanos y los expertos en tecnología, quienes deben colaborar en la planificación, ejecución y evaluación de prácticas que fomenten el uso responsable de la IA.

En las pequeñas y medianas empresas (PYME), esto puede traducirse en prácticas básicas como talleres de sensibilización, guías éticas simples y revisión periódica de procesos. En cambio, las empresas grandes o multinacionales deben implementar marcos más rigurosos, como centros de excelencia, auditorías internas, políticas de gobernanza tecnológica y métricas de impacto ético.

La capacitación por sí sola no es suficiente; debe estar respaldada por cambios estructurales en procesos, incentivos y valores organizacionales que refuercen la importancia de la ética. Recursos humanos juega un rol clave al garantizar que las bases culturales estén alineadas con estos principios, liderando junto con la dirección y los equipos técnicos la creación de hábitos, prácticas y estructuras que permitan una integración de la IA que sea no solo efectiva, sino también justa, transparente y centrada en el bienestar humano.

Incorporar consideraciones éticas en procesos de evaluación y promoción

Establecer espacios seguros para discusión de dilemas éticos

Reconocer y premiar ejemplos destacados de implementación ética

Incluir la ética como criterio explícito en procesos de decisiones

Comunicar regularmente avances y compromisos éticos

Uso Ético en el Entorno Laboral

La IA como Herramienta de Colaboración Humana

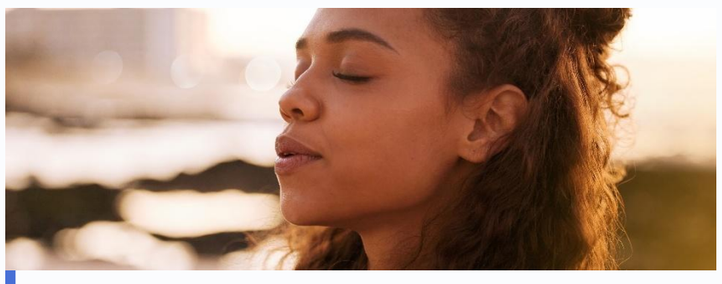
La implementación de sistemas de inteligencia artificial está transformando profundamente el entorno laboral, ofreciendo oportunidades para mejorar la productividad, la calidad y la satisfacción en el trabajo. Sin embargo, esta evolución también plantea desafíos éticos que deben abordarse de forma proactiva. El enfoque recomendado es concebir la IA como una herramienta de colaboración que amplifica las capacidades humanas y libera tiempo para tareas de mayor valor, promoviendo un paradigma de "IA colaborativa" que pone a las personas en el centro de la transformación digital.

Capacitación Adaptada

Desarrollar programas de capacitación que preparen a los colaboradores para trabajar con sistemas de IA, incluyendo formación para adquirir y actualizar habilidades, garantizando una transición justa y el uso de la IA como herramienta de empoderamiento.

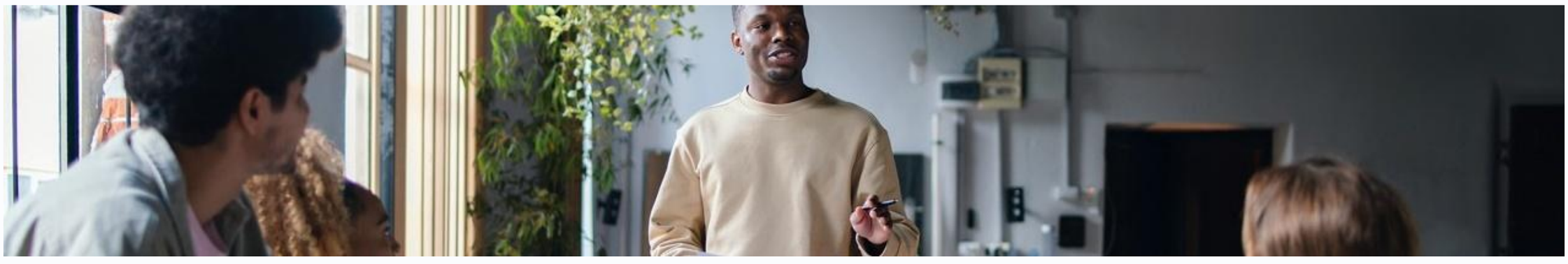
Diseño Participativo

Involucrar a colaboradores en el diseño e implementación de soluciones de IA que afectarán su trabajo, aprovechando su conocimiento del dominio y asegurando que la tecnología responda a necesidades.



Bienestar Laboral

Monitorear y gestionar proactivamente el impacto de la IA en el bienestar psicológico, la autonomía y la satisfacción laboral de los empleados, evitando la intensificación excesiva del trabajo.



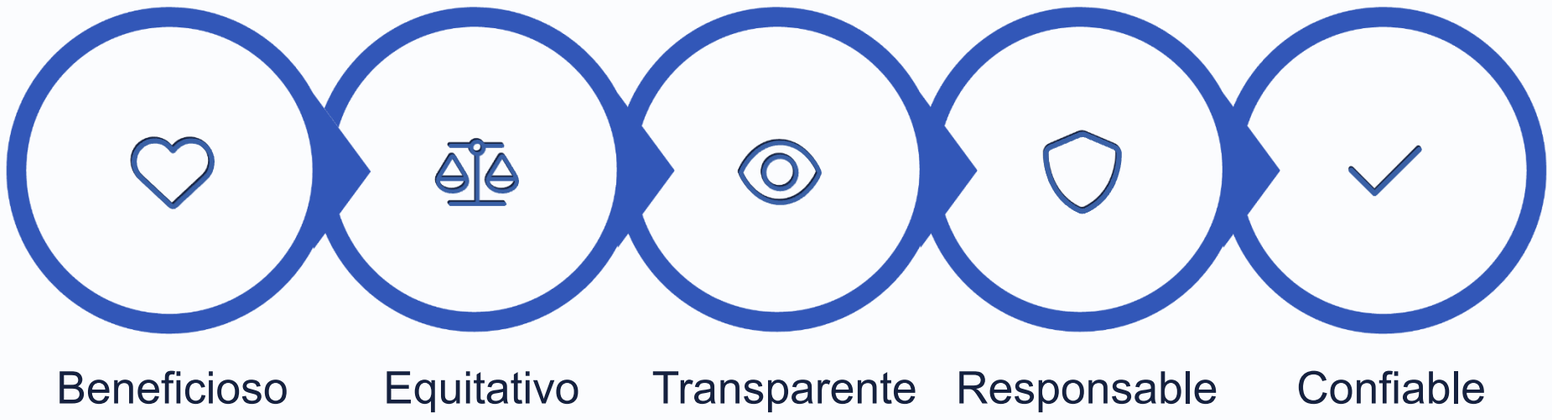
Buenas Prácticas para Empleados

La responsabilidad en el uso de la IA no recae exclusivamente en la dirección o los departamentos de tecnología. Todos los empleados que interactúan con estos sistemas deben desarrollar una comprensión básica de su funcionamiento y limitaciones, así como seguir principios éticos en su utilización diaria.

Principios Éticos Fundamentales

Los principios éticos fundamentales que deben guiar la implementación y uso de la Inteligencia Artificial en las empresas de AmCham Panamá se articulan en cinco dimensiones esenciales.

Estos principios se han formulado considerando los estándares internacionales y adaptándolos al contexto empresarial panameño.



Fuente: Dell Technologies

Beneficioso: Generar valor social

Los sistemas de IA deben diseñarse e implementarse para generar beneficios tangibles para las personas, las organizaciones, la sostenibilidad ambiental y la sociedad panameña. Se deben priorizar aplicaciones que mejoren el bienestar, evaluar sus impactos netos y considerar efectos a largo plazo más allá de los beneficios inmediatos.

Equitativo: Evitar sesgos y exclusión

La IA debe operar de forma justa para todos, sin perpetuar discriminaciones. Es clave mitigar sesgos en datos y algoritmos, garantizar accesibilidad, y evaluar su impacto en distintos grupos demográficos.

Transparente: Explicación y trazabilidad

La IA debe ser comprensible para usuarios y partes interesadas. Se debe documentar su funcionamiento, informar cuándo se utiliza, y explicar decisiones relevantes de forma clara.

Responsable: Responsabilidad institucional

Las organizaciones deben asumir la responsabilidad por el uso y efectos de la IA. Esto implica establecer mecanismos de supervisión humana, rendición de cuentas y asumir responsabilidad por decisiones automatizadas.

Confiable: Supervisión y respuesta

La IA debe funcionar de forma segura y conforme a lo previsto. Se requiere realizar pruebas rigurosas, monitoreo continuo, protocolos de respuesta a incidentes y revisiones periódicas del sistema.

Estos principios no deben considerarse aisladamente, sino como un marco integrado que guía todas las fases del desarrollo e implementación de sistemas de IA. Su aplicación requiere un compromiso institucional y la participación de equipos multidisciplinarios que aporten diversas perspectivas.

La adhesión a estos principios éticos fundamentales no sólo contribuye a mitigar riesgos legales y reputacionales, sino que también genera confianza entre clientes, empleados y la sociedad panameña, elementos esenciales para el éxito sostenible de cualquier iniciativa de IA.

MENSAJE CLAVE: La ética no debe ser un elemento adicional o posterior en la implementación de sistemas de IA, sino un componente central integrado desde el diseño inicial. Los principios éticos fundamentales son la base sobre la cual se construye una IA responsable, confiable y alineada con los valores de la sociedad panameña.

Privacidad y Seguridad

Protección de Datos en la Era de la IA

La protección de datos personales es un derecho fundamental, especialmente relevante en sistemas de inteligencia artificial que procesan grandes volúmenes de información. En Panamá, la Ley 81 de 2019 sobre Protección de Datos Personales en Panamá, vigente desde 2021, y reglamentada mediante el Decreto Ejecutivo 285 del 28 de mayo de 2021 exige que el tratamiento de datos se base en consentimiento informado, específico y revocable, y que se respeten los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). La normativa obliga a considerar todo el ciclo de vida de los datos —desde su recolección hasta su eliminación— y aplicar medidas técnicas y organizativas que garanticen su seguridad, confidencialidad y uso transparente.

Principios de Privacidad para IA

- **Minimización de datos:** Recolectar solo la información estrictamente necesaria para el propósito específico del sistema de IA.
- **Limitación de propósito:** Utilizar los datos únicamente para los fines declarados y consentidos.
- **Transparencia:** Informar claramente sobre qué datos se recopilan y cómo se utilizan.
- **Control del usuario:** Permitir a los individuos acceder, corregir y eliminar sus datos.
- **Privacidad por diseño:** Incorporar consideraciones de privacidad desde las primeras etapas de desarrollo.

Consideraciones Especiales para Datos Sensibles:
Los datos relacionados con salud, biometría, origen étnico, creencias religiosas, afiliación política, orientación sexual y la información genética, requieren protecciones adicionales y justificación clara para su uso en sistemas de IA.

Privacidad y Seguridad

Ciberseguridad para Sistemas de IA

Los sistemas de IA presentan vulnerabilidades específicas que requieren enfoques de seguridad adaptados. Las empresas deben implementar medidas técnicas y organizativas apropiadas para proteger tanto los datos utilizados por estos sistemas como los propios algoritmos y modelos.

1

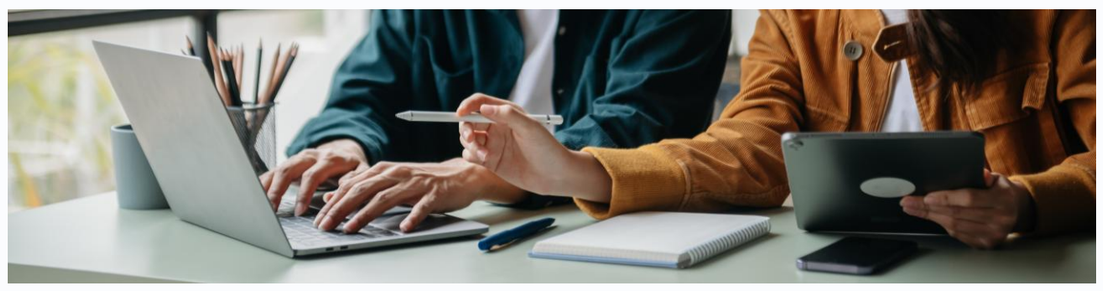
Protección contra Ataques Adversarios

Implementar defensas contra intentos deliberados de manipular los sistemas de IA mediante la introducción de datos maliciosos diseñados para provocar comportamientos incorrectos.

2

Seguridad de Modelos

Proteger los modelos de IA contra la extracción o inversión que podría comprometer datos sensibles utilizados en el entrenamiento o revelar secretos comerciales.



3

Monitoreo Continuo

Implementar sistemas de detección temprana de comportamientos anómalos que podrían indicar compromisos de seguridad o manipulación de los sistemas de IA.

4

Gestión de Acceso

Establecer controles estrictos sobre quién puede acceder, modificar o implementar sistemas de IA, especialmente aquellos que procesan información sensible o toman decisiones críticas.

Ciberseguridad para Sistemas de IA

A medida que los sistemas de IA se vuelven más poderosos y están más integrados en la sociedad, también aumentan los riesgos como la manipulación, el fraude y la pérdida de control humano. La OCDE* propone establecer **líneas rojas para la IA**, es decir, **prohibiciones claras y aplicables** sobre usos peligrosos o poco éticos, como la vigilancia masiva, la suplantación de identidad, las armas autónomas y los comportamientos engañosos. Estas restricciones deben incorporarse desde el diseño de los sistemas, no solo aplicarse después de que ocurran daños, y requieren cooperación internacional para ser efectivas.

La gobernanza debe ser **proactiva**, con definiciones precisas, supervisión robusta y pruebas de que los sistemas no cruzarán esos límites, incluso en condiciones adversas. Estas líneas rojas son clave para generar confianza pública, prevenir riesgos claves y permitir una innovación segura y alineada con los valores humanos.

Advertencia importante: Las brechas de seguridad en sistemas de IA pueden exponer datos sensibles y permitir manipulaciones maliciosas, con consecuencias graves como pérdidas financieras, daño reputacional, discriminación o riesgos críticos en sectores como banca y salud.

Fuente: *OECD.AI

Carta de Derechos y Deberes Digitales

Compromiso organizacional con el uso ético de la Inteligencia Artificial

A medida que la inteligencia artificial (IA) se integra en los procesos laborales, las empresas tienen la responsabilidad de garantizar que su uso respete los derechos de los colaboradores, promueva la equidad y fortalezca la cultura organizacional. Esta carta establece los principios fundamentales, derechos y deberes que deben guiar la interacción con sistemas de IA en el entorno empresarial.

Principios Fundamentales

1. **Beneficioso:** debe aportar valor a las personas, organizaciones y sociedad panameña en su conjunto, sin reemplazar el juicio profesional.
2. **Equitativo:** debe operar sin sesgos, respectando la privacidad y protegiendo los datos personales.
3. **Transparente:** se debe informar cuando una interacción o decisión esté asistida por IA.
4. **Responsable:** las organizaciones deben asumir su responsabilidad por el uso y efectos de sus sistemas de IA.
5. **Confiable:** deben funcionar de manera fiable, segura y conforme a lo previsto.

Derechos de los Colaboradores

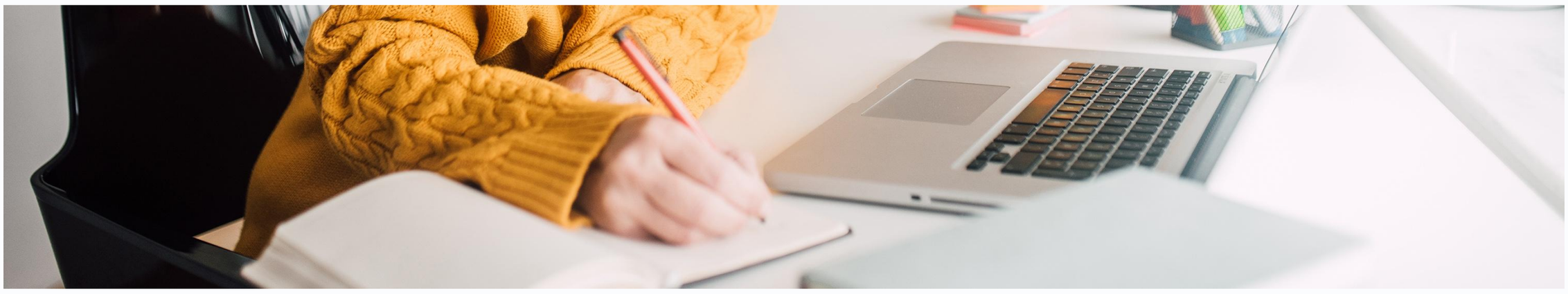
- Recibir asistencia de IA sin perder autonomía.
- Ser tratados de manera justa, sin sesgos ni discriminación.
- Que sus datos personales sean protegidos.
- Saber cuando se usa IA en decisiones.
- Usar sistemas de IA confiables y seguros.

Deberes de los Colaboradores

- Usar criterio, no depender ciegamente de la IA.
- Reportar sobre sesgos o usos indebidos.
- Validar resultados y proteger datos personales.
- Comunicar cuando se aplique IA en procesos.
- Capacitarse sobre el uso e impacto de la IA.

Responsabilidades de los Líderes y la Empresa

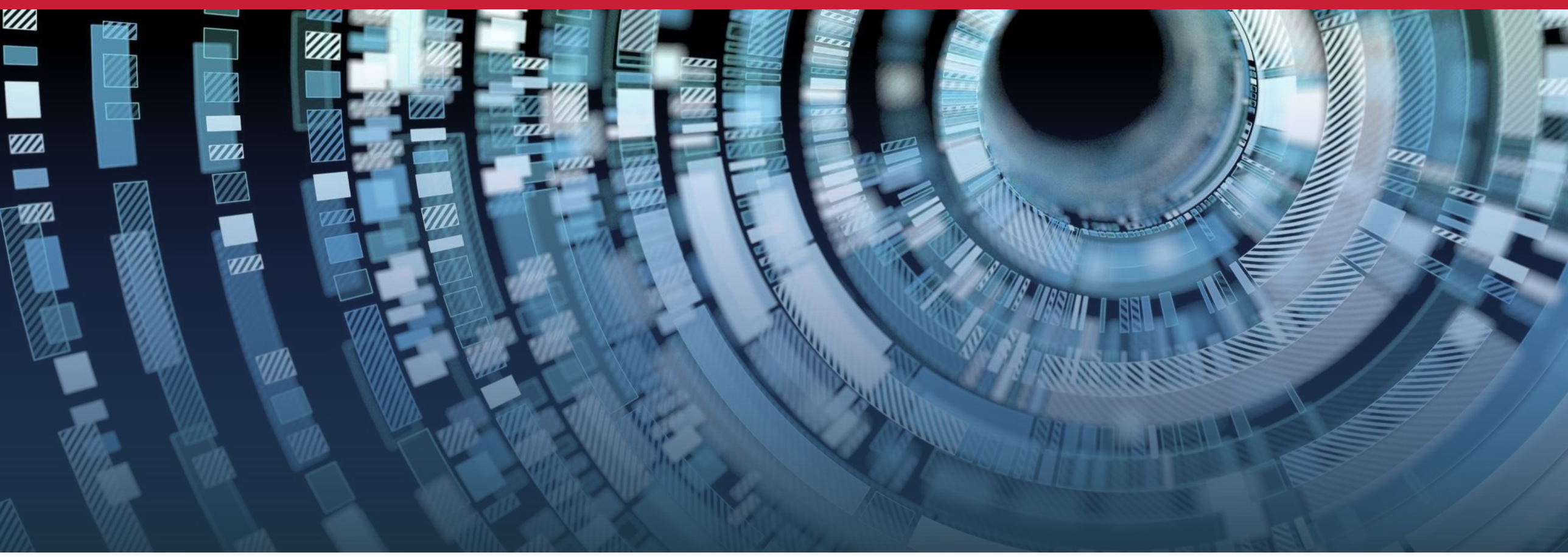
- Implementar IA que beneficie a la sociedad y respete el juicio profesional.
- Proteger la privacidad y el uso ético de la información.
- Desplegar sistemas seguros, preciosos y auditables.
- Definir políticas claras para el uso ético de la IA.
- Integrar principios de IA en la cultura organizacional.



Compromiso Final

Como organización, nos comprometemos a cumplir y promover los principios establecidos en esta Carta de Derechos y Deberes Digitales, asegurando que el uso de la inteligencia artificial en nuestros procesos respete la ética, la transparencia y el bienestar de todas las personas que forman parte de nuestra comunidad laboral.

Innovación Responsable



IA como Motor de Competitividad Ética

La falsa dicotomía entre innovación y responsabilidad ha sido superada por una comprensión más madura del mercado actual: la innovación verdaderamente sostenible solo es posible cuando se desarrolla dentro de un marco ético sólido. Para las empresas panameñas, la adopción de IA responsable representa una oportunidad estratégica para diferenciarse tanto a nivel regional como global.

La innovación responsable no solo mitiga riesgos, sino que genera valor tangible a través de múltiples vías: mejora la confianza de clientes y colaboradores, reduce costos asociados a fallos éticos, facilita el cumplimiento regulatorio anticipado y abre nuevos mercados sensibles a consideraciones éticas.

> "*La innovación - cualquier idea nueva - por definición no será aceptada a la primera. Hacen falta intentos repetidos, demostraciones interminables, ensayos monótonos antes de que la innovación pueda ser aceptada e interiorizada por una organización. Esto requiere una paciencia valiente*.“
>
> — Warren G. Bennis, en Leaders: The Strategies for Taking Charge

Iniciativas para Fomentar una Cultura de Innovación Responsable

“Hackaton” Ético

Eventos donde equipos multidisciplinarios abordan desafíos éticos relacionados con productos y servicios de la empresa.

Premios a la Innovación Responsable

Reconocimiento formal a proyectos que destacan por su impacto positivo en la sociedad y el medio ambiente.

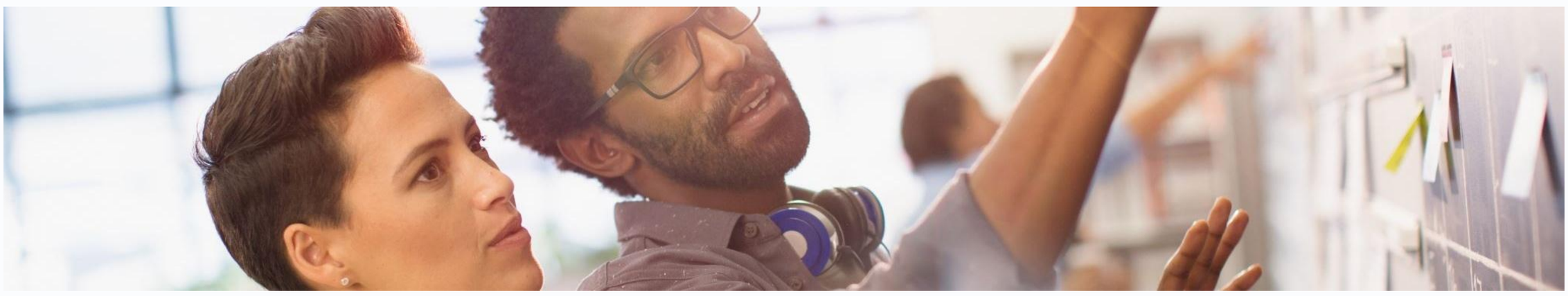
Alianzas Académicas

Colaboraciones con universidades, SENACYT o entidades regionales en innovación para incorporar perspectivas externas y mantener actualizados los estándares éticos.

Espacios Seguros

Canales donde los empleados pueden expresar preocupaciones éticas sin temor a represalias, fomentando la transparencia.

Innovación Responsable



Marco para la Innovación Responsable en IA

Ideación Ética

Incorporar consideraciones éticas desde la conceptualización, evaluando el propósito y potencial impacto de la solución de IA. Utilizar metodologías como “Ética por diseño" para anticipar implicaciones.

Desarrollo Inclusivo

Asegurar diversidad en equipos de desarrollo. Implementar prácticas como programación en pares ética, donde uno de los desarrolladores enfoca específicamente en consideraciones éticas.

Evaluación Multidimensional

Verificar no sólo la funcionalidad técnica, sino también el impacto social, la inclusividad y la alineación con valores organizacionales. Incluir pruebas con grupos diversos de usuarios.

Despliegue Gradual

Implementar sistemas primero en entornos controlados, con supervisión humana significativa. Escalar solo después de validar comportamiento ético en condiciones reales.

Monitoreo Continuo

Establecer sistemas para detectar impactos inesperados o derivas éticas incluyendo revisiones éticas en cada fase de proyectos de IA. Mantener canales abiertos para retroalimentación de usuarios y públicos de interés.

Mejora Iterativa

Incorporar lecciones aprendidas para refinar tanto el sistema como el proceso de desarrollo. Compartir aprendizajes con la comunidad cuando sea apropiado.

Beneficio estratégico: Las empresas que adoptan un enfoque de innovación responsable en IA no solo minimizan riesgos, sino que también suelen desarrollar soluciones más robustas, adaptables y alineadas con las necesidades reales del mercado, lo que puede traducirse en ventajas competitivas significativas a largo plazo.

Caso Ilustrativo: Sistema de Evaluación de Desempeño

La **Superintendencia de Bancos de Panamá** ha implementado **inteligencia artificial para fortalecer la supervisión financiera**, utilizando más de 200 tableros de analítica. Aunque no se aplica directamente a la evaluación de desempeño individual, la IA ha permitido liberar a los empleados de tareas rutinarias, mejorando su enfoque en análisis de valor agregado.

Esta transformación apoya indirectamente una gestión más ética y eficiente del talento humano.

Fuente: La Estrella de Panamá / BID – Programa GerencIA Panamá

3.2 Implementación

Gobernanza de la IA

Una gobernanza efectiva de la inteligencia artificial requiere un enfoque centrado en el ser humano, donde las personas mantengan control significativo sobre el diseño, implementación y uso de estos sistemas. Esto implica que, sin importar el nivel de automatización, las decisiones clave sobre objetivos, límites éticos y criterios de éxito deben seguir siendo responsabilidad humana.

Lejos de oponerse al avance tecnológico, este enfoque busca asegurar que la IA amplifique el potencial humano sin sustituir el juicio ético, y que las empresas adopten marcos de gobernanza que reflejen claramente esta priorización de valores.

1

Visión y Propósito

Definición de objetivos éticos y de negocio para la IA

2

Políticas y Directrices

Normas específicas para desarrollo, adquisición y uso de IA

3

Roles y Responsabilidades

Estructura organizacional clara con compromisos definidos

4

Procesos y Controles

Mecanismos de supervisión, auditoría y gestión de riesgos

5

Cultura Organizacional

Valores compartidos, capacitación y concientización

Gobernanza de la IA

Supervisión y Control: Estructuras Organizativas

La implementación efectiva de principios éticos requiere estructuras organizativas dedicadas con autoridad real para influir en decisiones de negocio. Dependiendo del tamaño y la complejidad de la organización, estas estructuras pueden variar, pero deben compartir características fundamentales:

Estructura	Composición Recomendada	Responsabilidades Principales
Comité de Ética de IA (sugerido para PYMES)	Alta dirección, especialistas técnicos, expertos en ética, representantes legales y de diversas áreas del negocio. El Observatorio de Implicaciones Sociales y Éticas de la IA (OECD por sus siglas en inglés) sugiere alinear la estructura del comité con el ciclo de vida de IA.	Establecer políticas generales, resolver dilemas éticos complejos, aprobar usos de alto riesgo, mitigar riesgos, manejo de incidentes
Oficina de Gobernanza de IA	Gerente de ética digital, oficiales de cumplimiento, analistas de riesgo, especialistas en privacidad de datos	Implementar políticas, gestionar evaluaciones de impacto internas y externas, monitorear cumplimiento, coordinar capacitaciones
Red de Campeones de IA Ética	Empleados de diversos departamentos con interés en ética digital	Promover buenas prácticas, identificar problemas potenciales, servir como primer punto de contacto
Centro de Excelencia (COE) de IA** (sugerido para empresa con recorrido avanzado en transformación digital)	Alta dirección, especialistas en IA y ciencias de datos, expertos en ética y regulación, representantes de recursos humanos y formación, delegados de áreas operativas y de negocio, auditoria externa y cumplimiento, voz del usuario o cliente	Establecer políticas, garantizar transparencia y trazabilidad, promover una cultura de ética digital, y facilitar la adopción de IA alineada con los objetivos estratégicos, sociales y ambientales.

**Fuente: Microsoft

Una gobernanza efectiva en inteligencia artificial requiere acceso directo a la alta dirección para priorizar la ética sobre intereses comerciales. Es clave colaborar con proveedores, clientes, reguladores y la comunidad mediante iniciativas sectoriales y diálogos abiertos. También se deben impulsar procesos de estandarización que fortalezcan prácticas éticas. Se propone alinear el comité de ética de IA con el ciclo de vida de los sistemas. Esto permite supervisión ética desde el diseño hasta el monitoreo continuo.

Recomendaciones para Implementación

Hoja de Ruta Práctica

La implementación de un marco ético para IA puede parecer abrumadora, especialmente para organizaciones que recién inician su transformación digital. Para facilitar este proceso, se propone una hoja de ruta gradual y adaptable según el tamaño, sector, madurez digital y complejidad tecnológica de cada empresa.

Esta metodología, diseñada para el contexto panameño, considera limitaciones comunes en recursos técnicos, el marco regulatorio en evolución y las particularidades culturales del entorno empresarial. Los plazos sugeridos dependerán directamente del nivel de preparación y sofisticación de los sistemas de IA utilizados.

Factores Críticos de Éxito

- **Compromiso** visible de la alta Dirección
- Asignación adecuada de **recursos**
- **Enfoque** multidisciplinario (no solo técnico)
- Participación de **audiencias diversas**
- Mentalidad de **mejora continua**

Las empresas deben adaptar sus prácticas según su tamaño:
PYMES: Capacitación básica, guías prácticas, revisión manual, comité de ética de IA y asignar roles y responsabilidades a puestos ya existentes.
Grandes empresas y/o Multinacionales: Políticas robustas, oficina de gobernanza de IA, red de campeones de IA, centro de excelencia, auditorías externas y métricas.

Etapas de Implementación

Fase 1: Fundamentos

Duración estimada: 1-3 meses

- Establecer compromiso formal con IA ética (principios fundamentales y carta de derechos y deberes)
- Identificar y mapear sistemas de IA existentes y planificados
- Formar equipo multidisciplinario inicial de gobernanza
- Realizar capacitación de concientización básica y para líderes

Fase 2: Estructuración

Duración estimada: 2-4 meses

- Desarrollar políticas y directrices específicas para IA
- Implementar evaluaciones de impacto ético Establecer roles y responsabilidades formales
- Iniciar capacitación por rol, incluyendo formación en responsabilidad y rendición de cuentas

Fase 3: Operacionalización

Duración estimada: 3-6 meses

- Integrar consideraciones éticas en procesos de Desarrollo
- Implementar mecanismos de monitoreo continuo
- Establecer canales de retroalimentación para usuarios
- Desarrollar protocolos de respuesta a incidentes

Fase 4: Maduración

Duración estimada: Continua

- Realizar revisiones y/o auditorías éticas internas y externas
- Refinar políticas basadas en experiencia acumulada
- Compartir mejores prácticas con el ecosistema
- Participar en iniciativas de estandarización

Marco de Implementación Ética

Este marco guía el uso ético de la IA, adaptándose al contexto empresarial sin perder de vista los cinco principios fundamentales. Debe integrarse con procesos de cumplimiento normativo, como la Ley 81 de 2019 sobre Protección de Datos Personales en Panamá. El objetivo no busca la perfección inmediata, sino un compromiso con la mejora continua, equilibrando la innovación y responsabilidad.

Principio	Preguntas Clave	Acciones de Gobernanza Recomendadas	Departamentos Involucrados
Beneficioso	• ¿Cómo mejora el sistema el bienestar humano? • ¿Se han evaluado los beneficios netos para todos los públicos de interés?	❑ Realizar evaluaciones de impacto previo a la implementación de la IA ❑ Definir métricas de beneficio social ❑ Recopilar retroalimentación continua de usuarios ❑ Documentar riesgos éticos por caso de uso	• Innovación • RSE/Sostenibilidad/ ASG • Planificación Estratégica • Experiencia de Cliente
Equitativo	• ¿El sistema trata a todos los usuarios de manera justa? • ¿Se han identificado y mitigado posibles sesgos?	❑ Utilizar conjuntos de datos diversos y representativos ❑ Implementar pruebas de sesgo e imparcialidad ❑ Diseñar con accesibilidad en mente	• Recursos Humanos • Diversidad e Inclusión • TI • Desarrollo de Producto
Transparente	• ¿Pueden los usuarios comprender cómo y por qué el sistema de IA toma ciertas decisiones? • ¿Se comunica claramente cuándo se está interactuando con IA?	❑ Documentar las fuentes de datos, características y limitaciones del modelo. ❑ Desarrollar documentación clara sobre el funcionamiento de los sistemas ❑ Implementar interfaces que expliquen las decisiones de la IA ❑ Divulgar proactivamente el uso de IA en las interacciones con clientes	• Legal / Cumplimiento • TI • Marketing • Atención al Cliente
Responsable	• ¿Quién es responsable de las decisiones del sistema? • ¿Cómo se rastrean y corrigen los errores?	❑ Definir claramente roles y responsabilidades ❑ Implementar sistemas de trazabilidad de decisiones ❑ Establecer protocolos de respuesta a incidentes ❑ Definir criterios específicos para determinar cuándo las decisiones automatizadas requieren revisión humana	• Legal • Gestión de Riesgos • Alta Dirección • Operaciones • TI | Desarrollo de Software
Confiable	• ¿Puede auditarse el funcionamiento del sistema? • ¿Existen mecanismos para validar resultados?	❑ Implementar registros detallados y auditables ❑ Permitir auditorías externas. ❑ Diseñar sistemas explicables. ❑ Revisar el desempeño regularmente. ❑ Definir indicadores éticos. ❑ Asignar responsables por cada modelo. ❑ Incluir cláusulas de responsabilidad en contratos.	• Auditoría Interna • TI Desarrollo de Software • Cumplimiento • Calidad

Punto importante:
La implementación efectiva de estos principios requiere una colaboración interdepartamental y un compromiso desde la alta dirección. No es responsabilidad exclusiva del departamento de TI, sino de toda la organización.

Gestión de Incidentes con IA

Preparación para lo Inevitable

Incluso con las mejores prácticas preventivas, los incidentes relacionados con IA son inevitables debido a su complejidad, naturaleza probabilística y entorno cambiante.

Un incidente de IA puede definirse como cualquier evento donde un sistema de IA produce resultados inesperados o indeseados que tienen el potencial de causar daños significativos a individuos, grupos, a la organización o a la sociedad en general. Estos pueden incluir decisiones discriminatorias, violaciones de privacidad, fallas de seguridad o comportamientos algorítmicos imprevistos.

Tipos de Incidentes de IA

- **Incidentes de precisión:** se generan resultados incorrectos o imprecisos
- **Incidentes de equidad:** se discrimina contra ciertos grupos
- **Incidentes de privacidad:** Exposición inadecuada de datos sensibles
- **Incidentes de seguridad:** Manipulación o compromiso del Sistema
- **Incidentes de transparencia:** Imposibilidad de explicar decisiones críticas

Protocolo de Respuesta a Incidentes de IA

Detección y Alerta

- Implementar sistemas automatizados de monitoreo que identifiquen patrones anómalos.
- Establecer canales de reportes para empleados y usuarios externos.
- Definir criterios de escalamiento según la severidad del incidente.

Contención y Evaluación

- Activar el equipo de respuesta multidisciplinario.
- Implementar medidas inmediatas para limitar el daño (que pueden incluir la suspensión temporal del sistema).
- Determinar el alcance y causa raíz del incidente.
- Documentar toda la información relevante.

Respuesta y Mitigación

- Desarrollar e implementar soluciones técnicas.
- Notificar a los afectados según normas legales y éticas.
- Coordinar comunicaciones a través de un correo electrónico compartido.
- Implementar medidas de remediación cuando sea necesario.

Recuperación y Aprendizaje

- Restaurar operaciones de forma segura.
- Analizar el incidente en detalle.
- Implementar mejoras en sistemas, procesos y políticas.
- Compartir aprendizajes internamente y, si aplica, externamente.

Equipo de Respuesta de Incidentes con IA

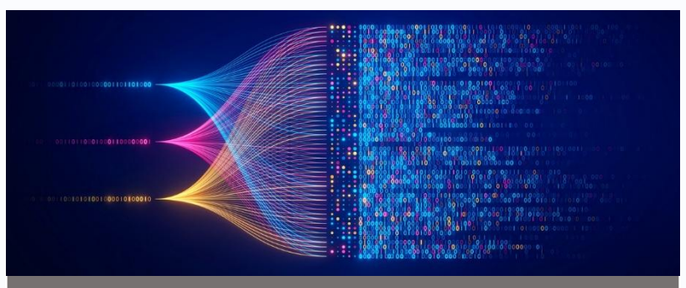
Responsabilidades del Equipo

La efectividad de la respuesta depende en gran medida de tener un equipo multidisciplinario preestablecido con responsabilidades claramente definidos. Las empresas deben adaptar sus prácticas al tamaño de sus equipos de trabajo. El enfoque sugerido es definir las responsabilidades y asignarlas entre personas que ya ocupan funciones clave en la empresa.

Abajo una sugerencia práctica:

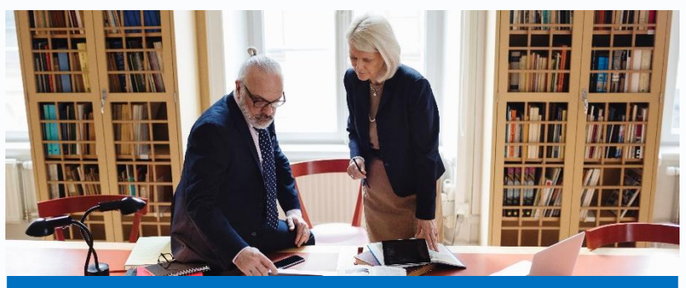
Coordinador de Incidentes

Lidera la respuesta general, coordina entre departamentos y toma decisiones críticas



Expertos Técnicos

Analizan el comportamiento del sistema, identifican causas técnicas y desarrollan soluciones



Asesor Legal / Cumplimiento

Evalúa implicaciones legales y obligaciones de divulgación

Especialista en Ética de IA

Evalúa el impacto ético y asegura que la respuesta se alinee con valores organizacionales.

Comunicaciones

Gestiona comunicaciones internas y externas sobre el incidente.

Representante de Negocio

Evalúa el impacto en operaciones comerciales y relaciones con clientes.

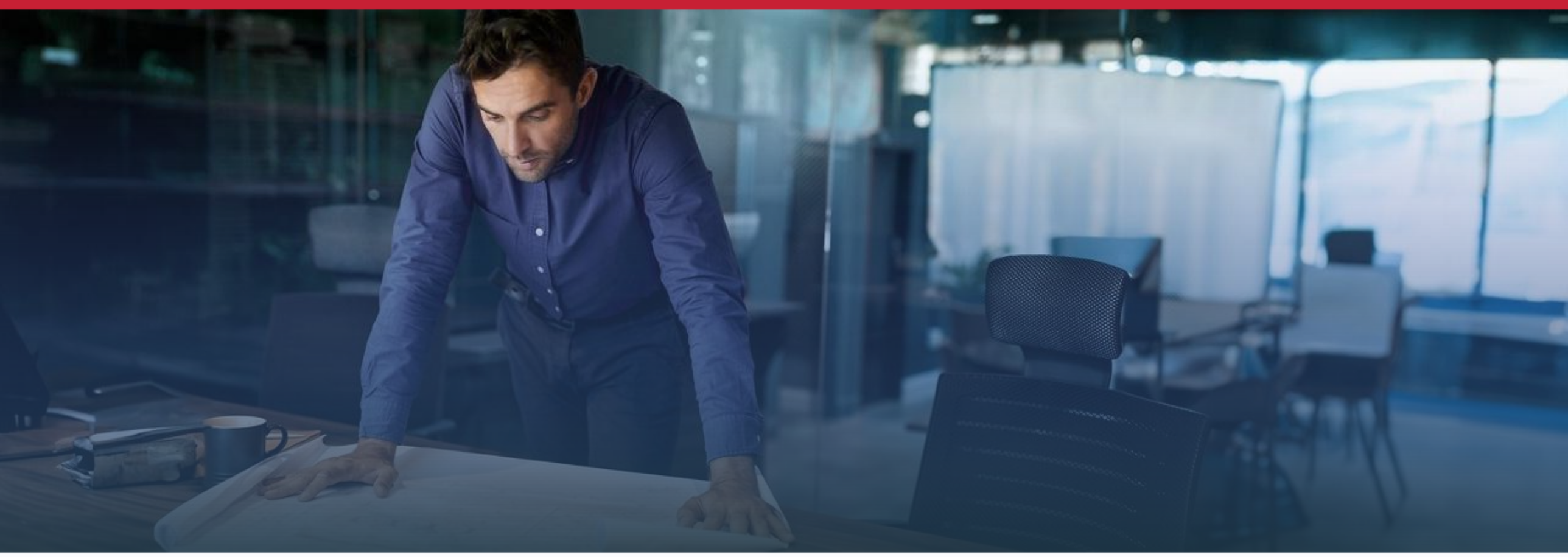
Para empresas panameñas, especialmente aquellas que están comenzando su implementación de IA, este enfoque estructurado para la gestión de incidentes puede parecer excesivo. Sin embargo, la experiencia internacional* demuestra que la preparación anticipada reduce significativamente el impacto negativo cuando ocurren problemas y contribuye a una adopción más confiada y exitosa de estas tecnologías transformadoras.

Fuente: AI Action Summit

Caso Ilustrativo: ¿Qué ocurre cuando los algoritmos de IA tienen sesgos?

Aunque no hay registros documentados de casos en Panamá, en otros países se han evidenciado impactos negativos cuando los sistemas de IA se entrenan con datos históricos sesgados. Por ejemplo, algoritmos de reclutamiento que favorecen a ciertos perfiles, como hombres en roles técnicos; sistemas de reconocimiento facial con mayores tasas de error al identificar personas de grupos raciales específicos; o plataformas de publicidad que muestran empleos mejor remunerados con más frecuencia a hombres que a mujeres, aun cuando sus perfiles son similares. Estos casos demuestran cómo la IA puede aprender y replicar patrones discriminatorios, perpetuando desigualdades económicas y limitando el desarrollo de grupos subrepresentados.

Confiabilidad



Fundamentos de la Confiabilidad en IA

La confiabilidad de un sistema de IA se refiere a su capacidad para funcionar de manera consistente, precisa y segura en las condiciones previstas de uso, así como para manejar adecuadamente situaciones imprevistas. En entornos empresariales, especialmente en sectores críticos como finanzas, salud o infraestructura, la confiabilidad no es negociable.

Un sistema de IA confiable debe demostrar robustez técnica, seguridad y precisión verificable. Esto implica que el sistema debe funcionar según lo esperado no solo en condiciones ideales, sino también cuando enfrenta datos atípicos, intentos de manipulación o cambios en el entorno de operación.

Dimensiones de la Confiabilidad

Precisión y Consistencia

Los sistemas de IA deben proporcionar resultados precisos y consistentes en el tiempo, dentro de los parámetros de operación para los que fueron diseñados. Esto requiere pruebas exhaustivas y monitoreo continuo.

Robustez

La capacidad del sistema para mantener un funcionamiento adecuado incluso en condiciones imprevistas o adversas, resistiendo intentos de manipulación o ataques maliciosos que puedan comprometer sus resultados.

Supervisión Humana

Establecer mecanismos adecuados de supervisión humana, especialmente en decisiones de alto impacto, garantizando que siempre exista la posibilidad de intervención humana cuando sea necesario.

Trazabilidad

Trazabilidad: El Fundamento de la Responsabilidad

La trazabilidad permite comprender cómo un sistema de IA llegó a una determinada conclusión o recomendación, facilitando la identificación de errores, la asignación de responsabilidades y la mejora continua. Un sistema trazable mantiene registros detallados de sus procesos de toma de decisiones, los datos utilizados y las intervenciones humanas realizadas.

1

Documentación de Datos

Mantener registros estandarizados y métricas éticas* sobre el origen, características y preprocesamiento de todos los datos utilizados para entrenar, validar y probar el sistema de IA, incluyendo metadatos sobre calidad y representatividad.

2

Registro de Modelos

Documentar la arquitectura, hiper parámetros, métodos de entrenamiento y métricas de evaluación de todos los modelos implementados, incluyendo versiones anteriores y justificaciones para los cambios realizados.

3

Logs de Decisiones

Implementar sistemas de registro que capturen los inputs recibidos, outputs generados, niveles de confianza y cualquier intervención humana en decisiones críticas, asegurando la capacidad de reconstruir el proceso decisorio.

4

Cadena de Custodia

Establecer procedimientos claros que documenten quién tuvo acceso al sistema, qué modificaciones realizó y bajo qué autoridad, creando una cadena de responsabilidad verificable desde el diseño hasta la implementación.

Recomendamos publicar el BOM (Lista de Componentes del Sistema), que detalla los datos, algoritmos y decisiones técnicas detrás de cada proceso de IA. Esta práctica refuerza la capacidad de explicar y transparencia, eliminando la percepción de “caja negra” y fortaleciendo la confianza de colaboradores, usuarios y reguladores.

Alerta Importante: Trazabilidad y Logs

La trazabilidad debe respetar estrictamente los lineamientos de privacidad y seguridad. Dado que los logs pueden filtrar datos, es crucial proteger el sistema central y sus integraciones. Para más detalles, consulte la **página 9** de esta guía.

Auditoría y Confianza

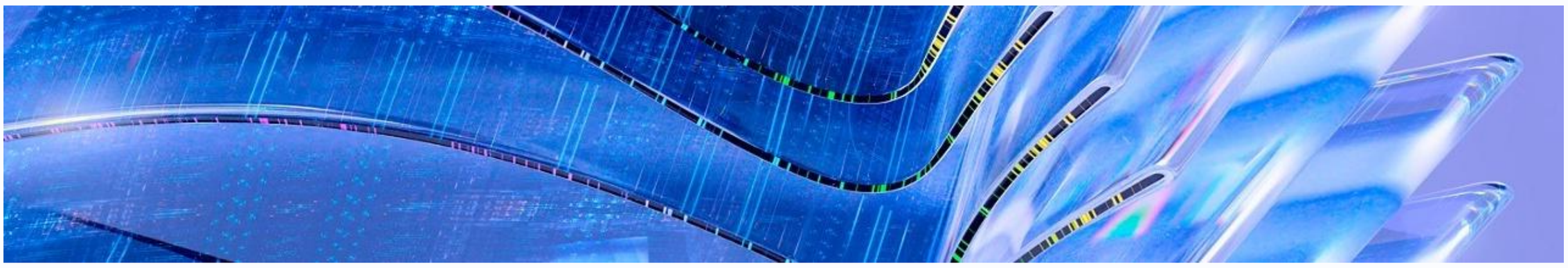
Las **auditorías y la documentación** estructurada son claves para garantizar la trazabilidad, confiabilidad y ventaja competitiva de los sistemas de IA, especialmente en sectores regulados en Panamá.

*Fuente: https://oecd.ai/en/

Marco Regulatorio Relevante

Panorama Regulatorio en Evolución

Aunque Panamá aún no cuenta con una regulación específica para la IA, las empresas deben atender normativas sectoriales vigentes y anticipar estándares internacionales emergentes, ya que el entorno regulatorio está en evolución y puede impactar tanto operaciones locales como transfronterizas.



Normativas Locales Relevantes

Ley 81 de 2019 de Protección de Datos Personales

Aunque su implementación completa está en proceso, esta ley establece principios fundamentales para el tratamiento de datos personales que tienen implicaciones directas para sistemas de IA, incluyendo requerimientos de consentimiento, finalidad, proporcionalidad y seguridad.

Regulaciones Sectoriales Bancarias

La Superintendencia de Bancos ha emitido directrices sobre tecnología financiera que afectan indirectamente el uso de IA en el sector, particularmente en relación con la gestión de riesgos, seguridad de la información y requisitos de transparencia hacia clientes.

Normativa de Ciberseguridad

La Ley 79 de 2021 sobre Delitos Cibernéticos y la Estrategia Nacional de Ciberseguridad establecen obligaciones que impactan la implementación de sistemas de IA, especialmente en aspectos relacionados con seguridad de datos y protección frente a vulnerabilidades.

Legislación sobre Propiedad Intelectual

El marco normativo panameño de propiedad intelectual, aunque no aborda específicamente la IA, establece principios relevantes para cuestiones como la titularidad de creaciones generadas por algoritmos y protección de algoritmos propietarios.

Normativa de Documentos Electrónicos

Ley 51 de 22 de julio de 2008, modificada por la Ley 82 de 9 de noviembre de 2012, define y regula documentos y firmas electrónicas y la prestación de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico

Legislación sobre Ciberdelincuencia

Ley 478 de 2025 modifica el Código Penal, el Código Procesal Penal y la Ley 11 de 2015, tiene como objetivo fortalecer la prevención, investigación y sanción de los delitos informáticos en Panamá, adecuando el marco legal a estándares internacionales y protegiendo a ciudadanos, empresas y entidades públicas frente a amenazas digitales

Marco Regulatorio Relevante

Enfoque Proactivo de Cumplimiento

Se recomienda a las empresas panameñas adoptar un enfoque proactivo que vaya más allá del cumplimiento mínimo legal, alineando el marco local con métricas internacionales como los indicadores comparables la Organización para la Cooperación y Desarrollo Económicos (OCDE).

Vigilancia Regulatoria

Monitorear activamente desarrollos regulatorios tanto locales como internacionales para anticipar cambios en el entorno normativo.

Participación Activa

Participar en consultas públicas y diálogos sobre nuevas regulaciones cuando sea posible, contribuyendo a la formación del marco normativo.

Adopción Anticipada

Implementar estándares internacionales reconocidos como buena práctica, incluso antes de que sean legalmente obligatorios en su jurisdicción.

Documentación Rigurosa

Documentar rigurosamente procesos de evaluación ética y decisiones de diseño para demostrar diligencia debida ante cualquier revisión.

Colaboración Sectorial

Colaborar con asociaciones sectoriales para desarrollar códigos de conducta autorregulatorios que eleven los estándares de la industria.

Protección de Datos

Incorporar prácticas robustas de **protección de datos** como parte integral de la estrategia de cumplimiento y ética digital.

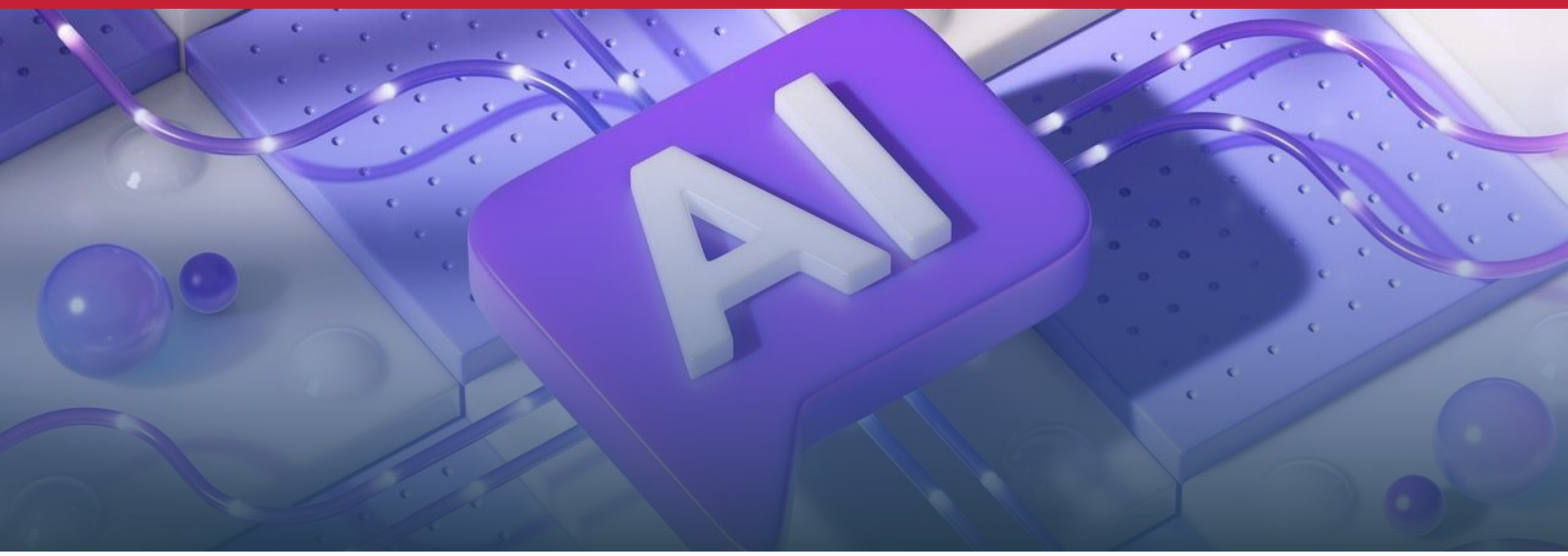
Recurso Recomendado: SENACYT formalizó la incorporación de Panamá a la Red Global para la Supervisión de la Inteligencia Artificial, una iniciativa liderada por la UNESCO que busca promover el uso responsable, ético y transparente de los sistemas de inteligencia artificial (IA) a nivel mundial. Se **recomienda a las empresas monitorear regularmente estas publicaciones** para mantenerse informadas sobre cambios en el entorno normativo panameño.

Estándares Internacionales Influyentes

Marco/Estándar	Organización	Relevancia para Empresas Panameñas
Marco Ético para IA	UNESCO	Primer instrumento normativo global sobre ética de IA, adoptado por Estados miembros incluyendo Panamá, establece principios que probablemente influenciarán futuras regulaciones locales.
Reglamento de IA (AI Act)	Unión Europea	Aunque no aplica directamente, establece un estándar global que podría afectar a empresas panameñas con operaciones en Europa o que forman parte de cadenas de valor globales.
Principios de IA	OCDE	Establece directrices adoptadas por numerosos países y que podrían servir como referencia para futura legislación panameña, especialmente considerando los esfuerzos del país por acercarse a estándares OCDE.
Estándar ISO/IEC 42001	ISO/IEC	Estándar emergente para sistemas de gestión de IA que probablemente se convertirá en referencia para certificaciones y buenas prácticas a nivel internacional.
Lineamientos Interamericanos de Gobernanza de Datos e Inteligencia Artificial	OEA	Establece un marco común para que los países de las Américas adopten modelos éticos, transparentes y colaborativos de gobernanza de datos e inteligencia artificial, que fortalezcan la toma de decisiones públicas, protejan los derechos humanos y promuevan el desarrollo sostenible y la innovación en la región

5.1 Conclusión

Compromiso con una IA Ética y Responsable



A lo largo de esta guía, hemos explorado los múltiples aspectos que conforman una implementación ética y responsable de la Inteligencia Artificial. Desde principios fundamentales hasta aplicaciones prácticas, hemos presentado un marco integral adaptado al contexto empresarial panameño, reconociendo tanto las oportunidades como los desafíos únicos que presenta esta tecnología transformadora.

La adopción de IA en Panamá se encuentra en un momento crítico. Las decisiones que tomemos hoy como comunidad empresarial determinarán si estas poderosas herramientas contribuirán a un desarrollo económico inclusivo y sostenible, o si amplificarán desigualdades existentes y generarán nuevos riesgos sociales.

> *"La inteligencia artificial es la última frontera. Debemos manejar esta tecnología con cuidado, con una visión clara de sus posibles consecuencias, y con un sentido de responsabilidad que nos haga conscientes de nuestros deberes para con las generaciones futuras."*
>
> — Mark Coeckelbergh, *Ética de la Inteligencia Artificial*

El Camino por Delante

93%

De las empresas globales líderes consideran que la ética será un factor competitivo crítico en la implementación de IA durante la próxima década

Fuente: Encuesta global realizada por UST AlphaAI Insights

78%

De los consumidores panameños indican que la confianza en el uso ético de sus datos influye significativamente en sus decisiones de compra

Fuente: PwC – Voice of the Consumer 2024 | 31 países, incluyendo Panamá

87%

De los empleados prefieren trabajar para organizaciones que implementan tecnología de manera responsable y centrada en el ser humano

Fuente: Boston Consulting Group (BCG) y MIT Sloan Management Review

5.1 Conclusión

Compromiso con una IA Ética y Responsable

Beneficios de la IA

Según estudios del **Banco de la Reserva Federal de San Luis** y el **Instituto Global McKinsey***, las empresas que adoptan IA han logrado mejoras del **20 al 30% en eficiencia operativa**, lo que se traduce en mayor competitividad y mejores márgenes. Y se preguntarán los líderes, qué se debe hacer con el tiempo que libera la IA. Las mejores prácticas sugieren:

- **Enfoque en iniciativas estratégicas:** Destinar el tiempo recuperado a optimizar procesos, impulsar la innovación, investigar el mercado o colaborar entre áreas.
- **Trabajo profundo y creatividad:** Concentrarse en tareas de alto valor como análisis, diseño y resolución de problemas.
- **Formación continua:** Usar el tiempo para adquirir o actualizar habilidades, mediante capacitación y certificaciones.
- **Relaciones humanas:** Fortalecer vínculos con clientes y equipos a través de atención personalizada, mentoría y colaboración.
- **Innovación ágil:** Probar nuevas tecnologías, desarrollar soluciones personalizadas y prototipar con mayor rapidez.
- **Bienestar personal:** Fomentar pausas, reducir horas extra y mejorar el equilibrio entre vida laboral y personal.

La inteligencia artificial (IA), gestionada con ética e inclusión, es una herramienta poderosa para los seres humanos. Mejora la eficiencia, la toma de decisiones y la personalización de productos y servicios, al tiempo que reduce costos operativos y libera carga laboral, impulsando la innovación y la competitividad en el mercado.

A nivel país, la IA puede cerrar brechas digitales en comunidades vulnerables, ampliar el acceso a servicios digitales y generar nuevas oportunidades de empleo y educación. Esto impulsa la productividad y el crecimiento económico, como indica el Foro Económico Mundial: un aumento del 10% en la penetración de banda ancha puede elevar el producto interno bruto (PIB) en países en desarrollo hasta en un 1.4%**.** Para lograrlo, es esencial invertir en infraestructura digital, formación tecnológica y marcos éticos que aseguren beneficios para toda la sociedad.

Para las empresas miembro de AmCham Panamá, adoptar este guía representa una oportunidad para:

Liderar con el ejemplo

Estableciendo estándares elevados que pueden influir positivamente en todo el ecosistema empresarial panameño, creando un efecto multiplicador en las prácticas responsables de IA.

Mitigar riesgos significativos

Legales, reputacionales y operacionales, anticipándose a potenciales problemas derivados del uso inadecuado de sistemas de IA y estableciendo protocolos preventivos.

Contribuir a posicionar a Panamá

Como un centro de innovación tecnológica responsable en la región, atrayendo talento, inversiones y oportunidades de colaboración internacional en el ámbito de la IA ética.

Construir confianza duradera

Con clientes, empleados, reguladores y la sociedad en general, lo que fortalece relaciones a largo plazo y mejora la reputación corporativa en un entorno cada vez más escrutado.

Crear valor sostenible

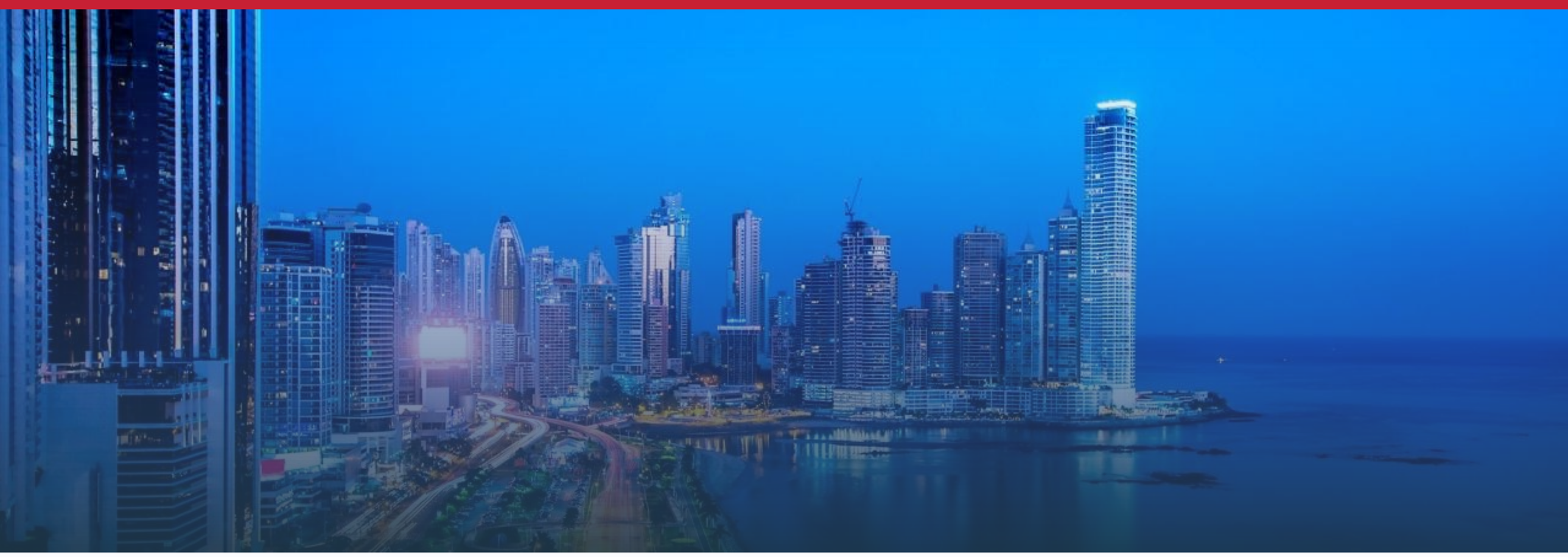
Que trascienda los beneficios financieros inmediatos, incorporando consideraciones éticas y sociales que aseguren impactos positivos a largo plazo para todos los grupos de interés.

El desarrollo ético de la inteligencia artificial es un proceso continuo que exige vigilancia, adaptabilidad y compromiso sostenido.

Esta guía es un punto de partida para que cada organización en Panamá desarrolle su propio enfoque de IA responsable, basado en valores como equidad, transparencia, privacidad y dignidad humana. El desarrollo ético de la IA requiere vigilancia y compromiso continuo para asegurar que esta revolución impulse el progreso inclusivo, el bienestar social y una competitividad sostenible.

Fuentes: https://itif.org/, McKinsey y Foro Económico Mundial

Casos de Uso en Panamá 2025



Aplicaciones Sectoriales con Impacto Local

La implementación de IA en Panamá está ganando impulso en diversos sectores, adaptándose a las particularidades del mercado local y aprovechando la posición estratégica del país como centro logístico, financiero y de servicios. Estos casos de uso demuestran cómo los principios éticos discutidos en esta guía pueden aplicarse en contextos específicos, generando valor mientras se gestionan adecuadamente los riesgos potenciales.

Banca y Finanzas

Los bancos panameños están implementando soluciones de IA para detección de fraude, evaluación crediticia y experiencia personalizada del cliente. Estas aplicaciones requieren especial atención a la equidad algorítmica para evitar discriminación en el acceso a servicios financieros, particularmente importante en un país con significativas disparidades socioeconómicas.

Fuente: PwC

Logística y Canal

Sistemas predictivos para optimización de tráfico marítimo, mantenimiento preventivo de infraestructura y gestión eficiente de recursos hídricos. La capacidad de explicar y transparencia son cruciales cuando estos sistemas impactan infraestructura crítica nacional, requiriendo un equilibrio entre eficiencia y supervisión humana significativa.

Fuente: Panacrypto

Salud

Aplicaciones de diagnóstico asistido, gestión hospitalaria y telemedicina potenciada por IA están emergiendo en el sistema de salud panameño. Estos sistemas deben implementarse con estrictas protecciones de privacidad y considerando las disparidades en acceso tecnológico entre áreas urbanas y rurales.

Fuente: IDrLpita.ai

Turismo

El sector turístico está adoptando IA para personalización de experiencias, gestión de reputación online y optimización dinámica de precios. Estas soluciones deben balancear la personalización con la protección de datos de visitantes internacionales, considerando las diversas expectativas culturales sobre privacidad.

Fuente: Prezi

Comercio Minorista

Minoristas panameños implementan IA para análisis de comportamiento del consumidor, gestión de inventario y marketing personalizado. La transparencia sobre la recopilación y uso de datos es fundamental para mantener la confianza del consumidor en un mercado altamente competitivo.

Fuente: Destino Panamá

Sector Público

Iniciativas de gobierno digital utilizan IA para mejorar servicios ciudadanos, optimizar procesos administrativos y analizar datos para políticas públicas. Estas aplicaciones requieren estricta gobernanza para asegurar equidad, transparencia y responsabilidad democrática.

Fuente: La Estrella

Casos de Uso en Panamá 2025

Estudio de Caso: IA en el Sector Bancario Panameño

En un estudio realizado por Forrester Consulting para Experian se revela cómo las empresas financieras están adoptando la inteligencia artificial generativa en distintos aspectos:

1

Experiencia del cliente

Creación de ofertas personalizadas de crédito y recomendaciones de productos que mejoran la satisfacción y generan mayores ingresos a través de la venta cruzada.

2

Enriquecimiento de modelos

Incorporación de datos no convencionales (redes sociales y análisis psicométricos) para evaluaciones de riesgo más completas, favoreciendo la inclusión financiera.

3

Eficiencia operativa

Automatizaciones que enriquecen el ciclo de vida del consumidor, optimizando procesos y generando ahorros significativos en las operaciones financieras.

4

Detección de fraude

Análisis de patrones y anomalías en grandes conjuntos de datos para identificar actividades potencialmente fraudulentas en tiempo real.

5

Servicio al cliente

Implementación de chatbots y herramientas que evolucionan para identificar problemas de los clientes y automatizar soluciones eficientes.

Fuente: Forrester Consulting

La Comisión de Economía Digital de la Cámara de Comercio Internacional (ICC) de Panamá realizó una encuesta sobre adopción de IA en empresas latinoamericanas revela una fuerte tendencia hacia su implementación en los próximos 12 meses, independientemente del tamaño o tipo de empresa. Los principales desafíos identificados son la falta de talento capacitado, la claridad de procesos y la inversión económica. Además, existe consenso sobre la necesidad de una regulación integral en Panamá, y una creciente conciencia sobre la gestión de datos, aunque aún con margen de mejora.

6.2 Apéndices

Referencias y Fuentes

Estándares y Marcos Internacionales

- UNESCO (2021). *Recomendación sobre la Ética de la Inteligencia Artificial*. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.
- OCDE (2019). *Principios de la OCDE sobre Inteligencia Artificial*. Organización para la Cooperación y el Desarrollo Económicos.
- Unión Europea (2021). *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre la Inteligencia Artificial*.
- ISO/IEC JTC 1/SC 42 (2023). *Artificial Intelligence Management System Standards*. International Organization for Standardization.
- Fondo Monetario Internacional – *¿Qué puede hacer la inteligencia artificial por la productividad estancada en América Latina y el Caribe?*
- US AID - *Guía Ética US AID*
- FATF – *Guía de Beneficiario Final*
- Banco Mundial – *Gobernanza Corporativa*
- OAS Lineamientos Interamericanos de Gobernanza de Datos e Inteligencia Artificial
- World Economic Forum (2025) - *Cómo la inteligencia artificial puede combatir la desigualdad | Foro Económico Mundial*

Fuentes Académicas y de Investigación

- Floridi, L., Cowls, J., Beltrametti, M., et al. (2021). *AI4People—An Ethical Framework for a Good AI Society*. Minds and Machines, 28(4), 689-707.
- Mittelstadt, B. (2019). *Principles Alone Cannot Guarantee Ethical AI*. Nature Machine Intelligence, 1(11), 501-507.
- Crawford, K., & Joler, V. (2020). *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Yale University Press.
- Universidad Tecnológica de Panamá (2025). *Transformando la educación en ingeniería: adaptaciones necesarias en la era de la inteligencia artificial*.

Recursos Corporativos

- Dell Technologies Principles for Ethical AI (2025)
- El Código de Ética de AMCHAM Panamá (2025)
- Microsoft (2022). *Responsible AI. Principles and approach*
- Google (2022). Responsible AI Principles
- World Economic Forum (2021). The AI Governance Journey: Development and Opportunities
- Asociaciones de Cámaras de Comercio Americanas (AACCLA). *Principios de la Cámara de Comercio de E.U. Sobre Inteligencia Artificial*

Recursos Locales

- Autoridad Nacional para la Innovación Gubernamental (2025). *Estrategia Nacional de Transformación Digital en Salud 2025-2030.*
- Superintendencia de Bancos de Panamá (2022). *Directrices para Implementación de Tecnologías Emergentes en el Sector Bancario.*
- Fundación Ciudad del Saber y SENACYT (2022). *Reporte sobre Ecosistema de Innovación en Panamá. Centro de Innovación.*
- Comisión de Economía Digital de la Cámara de Comercio Internacional Panamá (2025) *Informe - Adopción de Inteligencia Artificial en Empresas Latinoamericanas*
- Cámara Panameña de Tecnología (2025). *IA, Ética y Desarrollo Humano Regulación y Uso Sostenible para Panamá y Latinoamérica*

Sitios Web y Recursos Digitales Relevantes

Observatorio de Implicaciones Sociales y Éticas de la IA

https://oecd.ai/

Observatorio de la OCDE que proporciona investigación actualizada, métricas y buenas prácticas sobre implicaciones sociales y éticas de la IA.

Herramientas y Recursos Éticos de la IA

https://www.responsible.ai/

Colección de herramientas prácticas, plantillas y marcos teóricos para implementar IA ética en organizaciones de diversos tamaños y sectores.

Iniciativa Regional de IA para Latinoamérica

https://ilda.la

Plataforma colaborativa que adapta principios globales de IA ética al contexto latinoamericano, con casos de estudio relevantes para la región.

Esta lista de referencias no pretende ser exhaustiva, sino proporcionar un punto de partida para organizaciones que deseen profundizar en aspectos específicos de la IA ética. Se recomienda a las empresas mantenerse actualizadas sobre nuevas publicaciones y recursos, ya que este campo evoluciona rápidamente.

AmCham Panamá mantendrá una biblioteca digital actualizada de recursos adicionales, disponible para todas las empresas miembro a través de su portal web.

Glosario de Términos Clave

Este glosario proporciona definiciones claras y accesibles de términos técnicos y conceptos relacionados con la ética de la IA, para facilitar la comprensión por parte de lectores con diversos niveles de conocimiento técnico.

- **Inteligencia Artificial (IA)**

  Sistemas informáticos capaces de realizar tareas que normalmente requieren inteligencia humana, como percepción visual, reconocimiento de voz, toma de decisiones y traducción entre idiomas.

- **Aprendizaje Automático**

  Subcampo de la IA que permite a las computadoras aprender patrones a partir de datos sin ser explícitamente programadas para cada tarea específica.

- **Algoritmo**

  Conjunto de reglas o instrucciones definidas que conducen a la resolución de un problema o tarea específica.

- **Datos de Entrenamiento**

  Conjunto de información utilizada para enseñar a un sistema de IA a reconocer patrones y hacer predicciones o decisiones.

- **Sesgo Algorítmico**

  Resultados sistemáticamente prejuiciosos producidos por sistemas de IA, generalmente reflejando sesgos presentes en los datos de entrenamiento o en el diseño del algoritmo.

- **Caja Negra**

  Sistema de IA cuyo funcionamiento interno es opaco o difícil de entender, complicando la explicación de cómo llega a sus conclusiones.

- **Capacidad de Explicar**

  Capacidad de un sistema de IA para presentar los factores y lógica que influyen en sus resultados de manera comprensible para los humanos.

- **Humano en la cadena de decisión**

  Enfoque que mantiene supervisión humana significativa en sistemas automatizados, permitiendo intervención, validación o anulación de decisiones algorítmicas.

- **IA Generativa**

  Sistemas capaces de crear contenido original como texto, imágenes, música o videos basándose en patrones aprendidos de datos existentes.

- **Evaluación de Impacto Ético**

  Proceso sistemático para identificar, analizar y mitigar posibles impactos éticos negativos de un sistema de IA antes y durante su implementación.

- **Ataque adversarial**

  Manipulación deliberada de inputs para engañar a un sistema de IA y hacer que produzca resultados incorrectos o no deseados.

- **Privacidad por Diseño**

  Enfoque que incorpora protecciones de privacidad en cada etapa del desarrollo tecnológico, no como una consideración posterior.

Este glosario se complementará con recursos adicionales disponibles en línea, incluyendo videos explicativos y ejemplos prácticos para facilitar la comprensión de conceptos complejos. La terminología en el campo de la IA evoluciona rápidamente, por lo que se actualizará regularmente en la versión digital de esta guía.

Término	Definición
Aprendizaje Profundo	Subconjunto del aprendizaje automático basado en redes neuronales con múltiples capas que permiten modelar abstracciones complejas en los datos.
Alineamiento de Valores	Proceso de diseñar sistemas de IA para que actúen de manera consistente con valores humanos específicos y deseables.
Auditoría Algorítmica	Examen sistemático de un algoritmo para evaluar su funcionamiento, impacto y alineación con objetivos éticos y legales.
Drift Algorítmico	Fenómeno donde el rendimiento de un modelo de IA se degrada con el tiempo debido a cambios en el entorno o en los datos con respecto a las condiciones de entrenamiento.
Aprendizaje Federado	Técnica que permite entrenar modelos de IA en múltiples dispositivos o servidores descentralizados sin intercambiar los datos subyacentes, mejorando la privacidad.
Gobernanza de Datos	Conjunto de procesos, políticas, estándares y métricas que aseguran el uso efectivo y ético de los datos dentro de una organización.
Tokenización	Proceso de convertir datos sensibles en tokens no sensibles que mantienen el formato, pero no el valor original, protegiendo así la información.

Modelos de Políticas Internas

Modelos de Políticas Internas

Este apéndice proporciona modelos de políticas que las organizaciones pueden adaptar a sus necesidades específicas. Estos documentos han sido diseñados considerando las mejores prácticas internacionales pero adaptados al contexto legal y empresarial panameño.

Cada modelo de política incluye secciones obligatorias y opcionales, así como notas explicativas sobre cómo personalizarlas según el tamaño, sector y nivel de madurez digital de la organización. Se recomienda que estos documentos sean revisados por asesores legales internos antes de su implementación formal.

Instrucciones de Uso:
Estos modelos deben ser considerados como puntos de partida, no como documentos definitivos. Cada organización debe adaptarlos a su cultura, valores, procesos existentes y requisitos regulatorios específicos.

Modelo 1: Política de Gobernanza de IA

1

Propósito y Alcance

Define el propósito de la política, qué sistemas de IA están cubiertos, y a qué departamentos o unidades de negocio aplica. Establece la relación con otras políticas organizacionales existentes.

2

Principios Fundamentales

Articula los principios éticos centrales que guiarán todas las actividades relacionadas con IA en la organización, alineados con los valores corporativos y estándares internacionales.

3

Roles y Responsabilidades

Establece claramente quién es responsable de qué aspectos de la gobernanza de IA, incluyendo alta dirección, comités de supervisión, líderes técnicos, y todos los empleados que utilizan sistemas de IA.

4

Procesos de Aprobación

Detalla los procesos para evaluar, aprobar y monitorear proyectos de IA, incluyendo criterios para diferentes niveles de revisión basados en el riesgo e impacto potencial.

5

Requisitos de Documentación

Especifica qué documentación debe mantenerse para cada sistema de IA, incluyendo evaluaciones de impacto, decisiones de diseño, fuentes de datos, y métricas de rendimiento.

6

Mecanismos de Cumplimiento

Establece cómo se monitoreará el cumplimiento de esta política, incluyendo auditorías periódicas, indicadores clave, y consecuencias de no cumplimiento.

Modelos de Políticas Internas

Modelo 2: Procedimiento de Evaluación de Impacto Ético

Este documento proporciona una guía para evaluar los potenciales impactos éticos de un sistema de IA propuesto, documentar los hallazgos y determinar si se requieren medidas de mitigación antes de la implementación.

Sección	Contenido Principal	Personalización Necesaria
Cuestionario Inicial	Preguntas fundamentales sobre propósito, datos utilizados, autonomía del sistema y públicos de interés potencialmente afectados	Adaptar umbrales de riesgo según sector y tolerancia organizacional
Matriz de Riesgos Éticos	Marco teórico para evaluar probabilidad e impacto de diversos riesgos éticos potenciales	Ajustar categorías de riesgo según contexto específico del negocio
Requisitos de Consulta	Directrices sobre cuándo y cómo consultar con públicos de interés internos y externos	Especificar procesos de escalamiento según estructura organizacional
Plan de Mitigación	Modelo para documentar medidas para abordar riesgos identificados	Incorporar controles existentes y recursos disponibles
Proceso de Aprobación	Flujo de trabajo para revisión y autorización final	Alinear con niveles de autoridad y gobernanza existentes
Carta de Derechos y Deberes Digitales	Establece los principios que guían el compromiso de la empresa y orientan a sus colaboradores y líderes	Ajustar derechos y deberes según tamaño de la empresa.
Marco de Implementación Ética	Marco ético alineado con los cinco principios fundamentales y con normativas panameñas.	Alinear acciones y departamentos según tamaño de la empresa

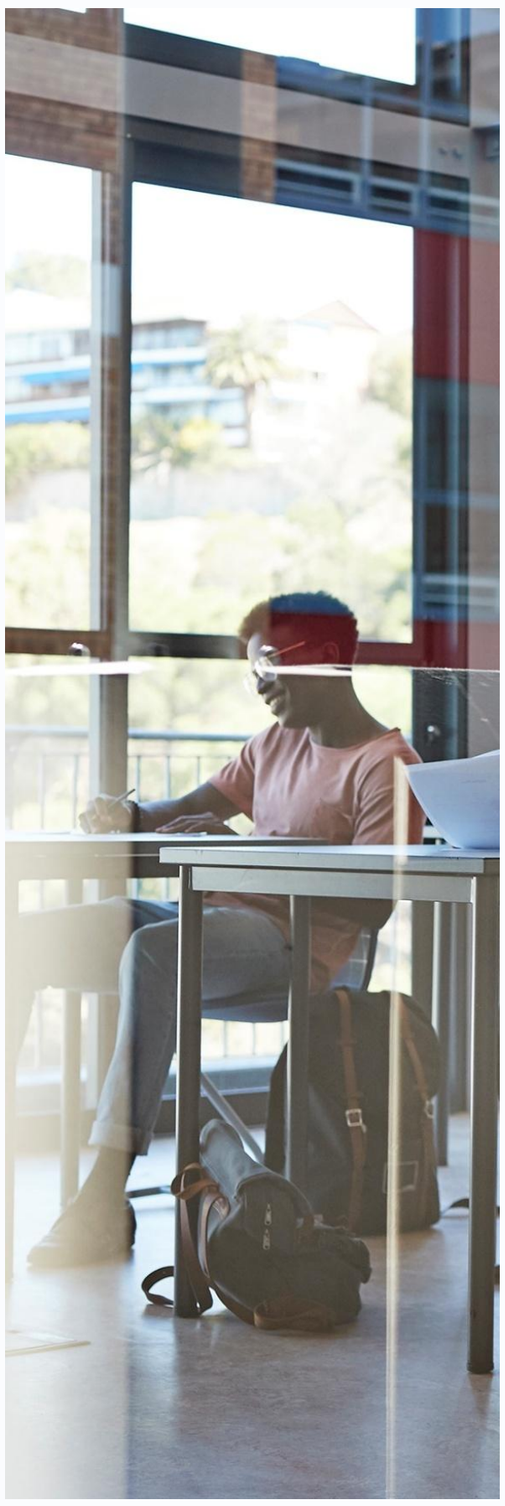
Estos modelos representan solo una muestra de las políticas que pueden ser necesarias para una implementación integral de IA ética. Otros documentos que las organizaciones deberían considerar desarrollar incluyen: Política de Privacidad de Datos para IA, Procedimiento de Auditoría Algorítmica, Directrices para Transparencia en IA, y Código de Conducta para Desarrolladores de IA.

Evaluación de Impacto Ético

Metodología Integral para Evaluar Sistemas de IA

La evaluación de impacto ético (EIE) es una herramienta esencial para identificar, analizar y mitigar riesgos éticos potenciales antes de implementar un sistema de IA. Similar a una evaluación de impacto ambiental o de privacidad, la EIE proporciona un proceso estructurado para considerar las implicaciones éticas de manera proactiva, documentada y rigurosa.

Esta metodología está diseñada para ser práctica y adaptable a diferentes contextos organizacionales, desde PYMES hasta grandes corporaciones, considerando las limitaciones de recursos y conocimientos especializados que pueden enfrentar las empresas panameñas.



Paso 1: Descripción del Sistema

Documentar el propósito, funcionalidad, datos utilizados, decisiones que tomará o influenciará el sistema, y públicos de interés potencialmente afectados. Esta fase establece el alcance de la evaluación.

Paso 2: Mapeo de Públicos de Interés

Identificar todos los grupos que podrían ser impactados por el sistema, prestando especial atención a grupos potencialmente vulnerables o subrepresentados en el proceso de desarrollo.

Paso 3: Identificación de Riesgos Éticos

Analizar sistemáticamente potenciales problemas éticos en categorías como equidad, transparencia, privacidad, autonomía, seguridad y bienestar. Utilizar técnicas como análisis de escenarios y revisión por pares.

Paso 4: Evaluación de Impacto

Estimar la probabilidad y severidad de cada riesgo identificado, considerando factores como número de personas afectadas, nivel de daño potencial, reversibilidad y duración de los efectos.

Paso 5: Medidas de Mitigación

Desarrollar estrategias específicas para abordar cada riesgo significativo, desde rediseño técnico hasta controles procedimentales, cambios en datos de entrenamiento o supervisión humana adicional.

Paso 6: Validación y Aprobación

Someter la evaluación a revisión por los responsables de gobernanza ética de IA en la organización, incorporar retroalimentación y obtener aprobación formal para proceder con la implementación.

Paso 7: Monitoreo Continuo

Establecer indicadores clave de desempeño ético (indicadores éticos) y procesos para monitorear continuamente el sistema después de su implementación, realizando nuevas evaluaciones cuando ocurran cambios significativos.

Evaluación de Impacto Ético

Herramienta de Evaluación: Matriz de Riesgos Éticos

La siguiente matriz puede utilizarse para sistematizar la identificación y priorización de riesgos éticos. Para cada dimensión, se evalúa el nivel de riesgo (bajo, medio, alto) y se documenta la justificación de esa calificación.

Dimensión Ética	Preguntas Clave	Nivel de Riesgo	Medidas de Mitigación
Equidad y No Discriminación	• ¿Podría el sistema generar resultados diferentes para distintos grupos demográficos? • ¿Los datos de entrenamiento son representativos de la población afectada?	Determinar según evaluación específica	A completar según riesgos identificados
Transparencia y Capacidad de Explicar	• ¿Pueden las decisiones o recomendaciones del sistema ser explicadas de manera comprensible? • ¿Está claro para los usuarios cuándo están interactuando con IA?	Determinar según evaluación específica	A completar según riesgos identificados
Privacidad y Protección de Datos	• ¿Qué datos personales procesa el sistema? • ¿Existe riesgo de identificación o de revelación inadvertida de información sensible?	Determinar según evaluación específica	A completar según riesgos identificados
Autonomía Humana	• ¿El sistema podría limitar indebidamente la capacidad de decisión de las personas? • ¿Existe supervisión humana significativa?	Determinar según evaluación específica	A completar según riesgos identificados
Seguridad y Fiabilidad	• ¿Qué nivel de daño podría causar el sistema si falla o es manipulado? • ¿Existen salvaguardas adecuadas?	Determinar según evaluación específica	A completar según riesgos identificados