MINISTERIO DE AMBIENTE Y ENERGÍA | GOBIERNO DE COSTA RICA | FONDO NACIONAL DE FINANCIAMIENTO FORESTAL

POLÍTICA INSTITUCIONAL

PARA EL USO DE INTELIGENCIA ARTIFICIAL

Elaborado por:

Unidad de Tecnologías de Información y Comunicación

LISTADO DE COLABORADORES

ELABORADA

Unidad de Tecnologías de Información y Comunicación

REVISADA

Dirección de Asuntos Jurídicos
Ministerio de Ciencia y Tecnología
Comité de Tecnologías de Información y Comunicación

APROBACIÓN

Jorge Mario Rodríguez Zúñiga Director General
Comité de Tecnologías de Información y Comunicación COTIC
Acuerdo No. DE-COTIC-SO-02-AC-02-2026

SIGLA

DG-UTIC-POL-001-2026-PIIA

Fecha

27/05/2026

VERSIÓN 1.3

TABLA DE CONTENIDO

1. OBJETIVO

Establecer los lineamientos institucionales para el uso, adopción, desarrollo y aprovechamiento responsable de tecnologías de Inteligencia Artificial (IA), garantizando su utilización ética, segura, transparente y alineada con los principios institucionales, la normativa nacional vigente y la Estrategia Nacional de Inteligencia Artificial (ENIA) 2024-2027 promovida por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT).

2. ALCANCE

La presente política es de acatamiento obligatorio para:

- Todas las personas funcionarias que presten servicios en el Fondo Nacional de Financiamiento Forestal y sus Fideicomisos.
- Personal contratado bajo la modalidad de servicios profesionales.
- Sistemas, plataformas o soluciones tecnológicas desarrollados o adquiridos por la Institución que incorporen componentes de Inteligencia Artificial.

Aplica tanto para herramientas institucionales como para herramientas externas utilizadas en el ejercicio de funciones laborales.

3. MARCO NORMATIVO Y REFERENCIAS

La presente política se fundamenta en:

- Constitución Política de la República de Costa Rica.
- Ley N° 6227 “Ley General de la Administración Pública”.
- Ley N° 8968 “Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales”.
- Principios de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre IA.
- Recomendación de la UNESCO sobre la Ética de la IA (2021)
- Estrategia Nacional de Inteligencia Artificial (ENIA) 2024-2027.
- Plan de Acción -ENIA Costa Rica 2024-2027.
- Normativa institucional relacionada con tecnologías de información, ciberseguridad, protección de datos y continuidad operativa.
- Política Institucional de Seguridad de la Información.

4. DEFINICIONES

Inteligencia Artificial (IA): Sistema basado en máquinas que, con objetivos explícitos o implícitos, infiere a partir de entradas recibidas cómo generar resultados tales como predicciones, contenido, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales.

IA Generativa: Tecnología de IA capaz de generar contenido nuevo como texto, imágenes, audio, video, código o análisis automatizados.

Supervisión Humana: Proceso por medio del cual una persona funcionaria realiza la revisión, validación y aprobación de los resultados generados por sistemas de inteligencia artificial, previo a su utilización oficial.

Datos Sensibles: Información relativa al fuero íntimo de la persona, como por ejemplo los que revelen origen racial o étnico, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida y orientación sexual, entre otros, conforme a la Ley N.° 8968 y su Reglamento.

Sesgo algorítmico: Ocurre cuando un sistema de inteligencia artificial o un algoritmo toma decisiones o genera recomendaciones que reflejan prejuicios existentes en los datos o en las reglas definidas por quienes lo diseñaron.

Explicabilidad: Capacidad de un sistema de inteligencia artificial para describir de manera comprensible los factores, datos y criterios que influyeron en la generación de un resultado o decisión.

Sistema de alto riesgo: Sistema de IA que, debido a la naturaleza de su finalidad o al impacto potencial de sus resultados, puede afectar de manera significativa a las personas, la organización o la prestación de servicios, requiriendo una evaluación, monitoreo y supervisión estrictos.

Decisión automatizada: Resultado o determinación generada por un sistema informático o de inteligencia artificial que influye o define una acción, recomendación o resolución, con limitada o nula intervención humana directa.

Alucinación / error de IA generativa: generación de contenido erróneo, impreciso o inventado por parte de un sistema de inteligencia artificial, presentado con apariencia de veracidad pese a no estar respaldado por información real o verificable.

5. PRINCIPIOS RECTORES PARA EL USO DE IA

La institución promoverá el uso de IA bajo los siguientes principios:

5.1 Ética y Responsabilidad

Toda solución de IA deberá utilizarse de manera ética, segura y responsable, procurando maximizar beneficios y minimizar posibles daños a las personas.

5.2 Transparencia

La transparencia se refiere a explicabilidad y divulgación sobre la lógica, los datos y las limitaciones del sistema.

5.3 Supervisión Humana

El contenido generado con apoyo de herramientas de Inteligencia Artificial deberá ser revisado, validado y aprobado por la persona funcionaria responsable antes de su uso oficial. La responsabilidad sobre la información publicada o utilizada recae siempre en el funcionario que la emite, independientemente de la herramienta utilizada para su elaboración.

5.4 Protección de Datos

El tratamiento de información mediante IA deberá respetar el derecho a la autodeterminación informativa, y demás derechos de la personalidad, la confidencialidad, privacidad y protección en el tratamiento de datos.

5.5 Inclusión y Equidad

La IA deberá utilizarse promoviendo accesibilidad, equidad, sostenibilidad y respeto a los derechos humanos.

5.6 Seguridad

Toda implementación de IA deberá considerar mecanismos de ciberseguridad, control de acceso y gestión de riesgos tecnológicos.

6. GOBERNANZA TECNICA INSTITUCIONAL DE IA

6.1 Coordinación Técnica

La rectoría nacional en ciencia, tecnología e IA corresponde al MICITT (Ley N.° 7169 y ENIA 2024-2027).

La Unidad de Tecnologías de Información y Comunicación será la dependencia responsable de emitir lineamientos técnicos relacionados con el uso institucional de IA, así como su coordinación con el Comité de Transformación Digital.

6.2 Evaluación de Herramientas

Toda herramienta de IA que procese información institucional deberá ser previamente evaluada y autorizada por la UTIC.

6.3 Coordinación Institucional

La implementación de soluciones de IA deberá coordinarse con las áreas de:

- **Asesoría Jurídica:** Brindará criterio sobre aspectos legales, regulatorios, propiedad intelectual, protección de datos, contratación administrativa, derechos de autor y demás obligaciones normativas aplicables.
- **Planificación Institucional:** Verificará la alineación de las iniciativas de IA con los objetivos estratégicos, planes institucionales, indicadores de gestión y procesos organizacionales.
- **Archivo Institucional:** Velará por el cumplimiento de la normativa archivística vigente, así como por la adecuada gestión, conservación, preservación y disposición de los documentos y registros generados o procesados mediante herramientas de IA.
- **Recursos Humanos:** Coordinará los procesos relacionados con capacitación, sensibilización, gestión del cambio, desarrollo de competencias digitales y aplicación de las disposiciones institucionales sobre el uso de la IA por parte del personal.

- **UTIC: Seguridad de la Información:** Evaluará los riesgos asociados al tratamiento de la información, verificará el cumplimiento de las políticas de ciberseguridad y protección de datos, y emitirá las recomendaciones técnicas necesarias para resguardar la confidencialidad, integridad y disponibilidad de la información institucional.

La coordinación con las áreas institucionales deberá realizarse de forma previa a la puesta en producción de cualquier solución de IA que procese información institucional, automatice procesos, apoye la toma de decisiones o genere productos que puedan tener efectos administrativos, legales, financieros o reputacionales para la institución.

7. USO RESPONSABLE DE HERRAMIENTAS DE IA

7.1 Uso Permitido

Las herramientas de IA pueden utilizarse para:

- Automatización de tareas administrativas en coordinación con la Unidad de Tecnologías de Información.
- Elaboración preliminar de documentos.
- Análisis preliminar de información que no implique un documento final.
- Optimización de procesos.
- Generación de resúmenes administrativos en el que no comprometa la estrategia institucional, ejecución presupuestaria y/o financiera. Así como información contractual de personal, PSA, Crédito y Convenios.
- Otras actividades compatibles con las funciones institucionales, siempre que su uso se ajuste a los principios, lineamientos y controles establecidos en la presente Política.

7.2 Validación Obligatoria

Todo contenido generado mediante IA deberá ser revisado y validado por el funcionario responsable antes de su uso oficial.

7.3 Uso Institucional

La utilización de IA deberá responder exclusivamente a fines laborales y alinearse con los objetivos institucionales.

8. PROTECCIÓN DE DATOS Y CONFIDENCIALIDAD

8.1 Información Restringida

Se prohíbe ingresar en herramientas o plataformas de inteligencia artificial que no cuenten con autorización institucional o con garantías adecuadas de protección y tratamiento de datos:

- Datos personales sensibles.
- Información confidencial
- Expedientes administrativos.
- Información financiera reservada.
- Credenciales, contraseñas o llaves de acceso.
- Cualquier otra información clasificada o sujeta a deberes de confidencialidad legal, contractual o institucional.

La restricción anterior aplica especialmente a plataformas abiertas al público o a servicios respecto de los cuales no existan garantías contractuales suficientes sobre el tratamiento de la información suministrada.

Excepcionalmente, el tratamiento de información institucional podrá realizarse en plataformas o entornos de IA expresamente autorizados por la Institución, siempre que cuenten con mecanismos de seguridad adecuados y condiciones contractuales que garanticen, entre otros aspectos, la protección de los datos, la limitación de su uso para entrenamiento de modelos, controles de retención y eliminación de información, así como el cumplimiento de la normativa aplicable en materia de seguridad y protección de datos.

8.2 Resguardo de Información

Toda interacción con herramientas de IA deberá cumplir con las políticas institucionales de seguridad de la información y protección de datos.

8.3 Almacenamiento y Trazabilidad

La institución establecerá mecanismos de auditoría, registro y trazabilidad del uso institucional de herramientas de IA.

9. TRANSPARENCIA Y SUPERVISIÓN HUMANA

9.1 Identificación de Contenido Generado por IA

Deberá indicarse mediante un pie de página que un contenido fue generado o asistido mediante IA en los casos en que dicho contenido tenga efectos hacia la ciudadanía, sustente actos administrativos o se difunda públicamente, conforme a la guía institucional.

Ejemplo: ***Contenido elaborado con asistencia de Inteligencia Artificial y revisado por personal institucional.***

9.2 Supervisión Obligatoria

Las recomendaciones, análisis o resultados generados por sistemas de inteligencia artificial no sustituyen el criterio técnico, jurídico, administrativo o de cualquier otra naturaleza de la persona funcionaria responsable, quien deberá, además, verificar la pertinencia, calidad y confiabilidad de las fuentes de información utilizadas por dichos sistemas antes de su uso oficial.

10. DESARROLLO Y ADQUISICIÓN DE SOLUCIONES DE IA

10.1 Evaluación Técnica

Toda solución institucional de inteligencia artificial deberá ser sometida a una evaluación técnica proporcional a su nivel de riesgo, la cual contemplará, como mínimo:

• Seguridad de la información.
• Protección de datos personales.
• Explicabilidad y trazabilidad de los resultados.
• Gestión de riesgos.
• Identificación, evaluación y mitigación de sesgos.
• Continuidad operativa.
• Evaluación de impacto algorítmico y, cuando corresponda, evaluación de impacto en la protección de datos.
• Calidad, integridad y gobernanza de los datos utilizados para entrenamiento, validación y operación.
• Gestión del ciclo de vida del sistema o modelo de IA, incluyendo su desarrollo, adquisición, implementación, actualización y retiro.

• Mecanismos de monitoreo, seguimiento y revisión periódica para detectar degradación del desempeño, cambios en el comportamiento del modelo u otros riesgos emergentes.

La Unidad de Tecnologías de Información y Comunicación (UTIC) mantendrá un Inventario Institucional de Sistemas de Inteligencia Artificial que registre todas las soluciones de IA desarrolladas, adquiridas o utilizadas por la institución.

La clasificación de riesgo permitirá aplicar medidas de supervisión, monitoreo y control proporcionales al impacto potencial de cada sistema, de conformidad con los principios de gestión de riesgos, seguridad de la información y protección de datos establecidos en esta Política.

10.2 Contratación de Servicios

Los procesos que realice la Institución para la adquisición, contratación o suscripción de herramientas y servicios de inteligencia artificial deberán incorporar criterios éticos, técnicos, jurídicos y de gestión de riesgos, alineados con la Estrategia Nacional de Inteligencia Artificial (ENIA) Costa Rica 2024-2027, la normativa vigente y las políticas institucionales aplicables.

Adicionalmente, los carteles, términos de referencia, contratos o acuerdos de servicio deberán contemplar, según corresponda y de forma proporcional al riesgo de la solución, aspectos relacionados con:

- La titularidad y protección de los datos institucionales y de los resultados generados por la herramienta.
- La prohibición o limitación del uso de información institucional para el entrenamiento o mejora de modelos de inteligencia artificial, salvo autorización expresa de la Institución.
- La ubicación, almacenamiento y transferencia de datos, considerando los requerimientos de seguridad y protección de la información aplicables. Los niveles de servicio, disponibilidad, continuidad operativa y soporte técnico.
- Las capacidades de auditoría, trazabilidad y rendición de cuentas sobre el funcionamiento de la solución.

- Los mecanismos de portabilidad, recuperación y eliminación de datos al finalizar la relación contractual.
- Las condiciones necesarias para reducir riesgos de dependencia tecnológica excesiva y facilitar la transición hacia soluciones alternativas cuando resulte necesario.

La UTIC, en coordinación con las áreas técnicas y administrativas competentes, podrá definir requisitos adicionales de seguridad, interoperabilidad, gobernanza y cumplimiento normativo según la naturaleza y el nivel de riesgo de la solución a contratar.

11. GESTIÓN DE RIESGOS Y SEGURIDAD

11.1. Gestión de Riesgos

La institución establecerá mecanismos para identificar, evaluar, mitigar y monitorear los riesgos asociados al uso de tecnologías de Inteligencia Artificial, incluyendo riesgos operativos, tecnológicos, éticos, legales, sesgos, reputacionales, intimidación y de ciberseguridad.

11.2. Seguridad de la Información

Toda herramienta de Inteligencia Artificial utilizada dentro de la institución deberá cumplir con los controles y lineamientos institucionales de seguridad de la información, ciberseguridad, protección de datos y continuidad operativa establecidos por la UTIC.

11.3 Uso de Herramienta Autorizada

La herramienta de Inteligencia Artificial autorizada para uso institucional es Microsoft Copilot, la cual viene incorporada en el Office 365 de cada funcionario y es una solución respaldada, desarrollada y administrada por Microsoft.

11.4. Uso de Herramientas No Autorizadas

Se prohíbe el uso de herramientas de Inteligencia Artificial no autorizadas por la institución para el procesamiento, análisis, almacenamiento o transferencia de información institucional sensible, confidencial o restringida.

Asimismo, no podrán utilizarse cuentas personales, aplicaciones externas o plataformas no aprobadas institucionalmente para tratar información relacionada con las funciones oficiales de la institución.

11.5. Monitoreo, Auditoría y Trazabilidad

La institución podrá implementar mecanismos de monitoreo, auditoría y trazabilidad sobre el uso de herramientas tecnológicas e Inteligencia Artificial utilizadas dentro de la infraestructura tecnológica institucional, con el fin de:

- Proteger la seguridad de la información;
- Prevenir fugas o uso indebido de datos;
- Verificar el cumplimiento normativo;
- Fortalecer la gestión de riesgos tecnológicos;
- Garantizar la supervisión humana;
- Mitigar riesgos asociados al uso inadecuado de tecnologías de IA.

La Unidad de Tecnologías de Información y Comunicación (UTIC) podrá realizar revisiones técnicas, análisis de registros, controles de acceso, monitoreo de aplicaciones, auditorías de seguridad y validaciones de cumplimiento relacionadas con el uso institucional de herramientas de inteligencia artificial.

Estas actividades deberán ejecutarse conforme a los principios de legalidad, necesidad, proporcionalidad, razonabilidad y finalidad legítima, limitándose a los fines institucionales de seguridad, cumplimiento normativo, gestión de riesgos y protección de la información. En ningún caso los mecanismos de monitoreo podrán utilizarse para fines distintos a los aquí establecidos ni implicar una vigilancia excesiva o desproporcionada de las personas funcionarias.

Toda actividad de monitoreo y tratamiento de información deberá realizarse de conformidad con la Ley N.° 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, la normativa institucional aplicable y los criterios jurisprudenciales vigentes en materia de protección de datos, privacidad y relaciones laborales.

11.6. Protección de Información Institucional

Los funcionarios deberán abstenerse de incorporar en plataformas públicas o no autorizadas de Inteligencia Artificial información que contenga:

- Datos personales;
- Expedientes administrativos;
- Información financiera;
- Documentos confidenciales;
- Credenciales de acceso;
- Información estratégica institucional;
- Cualquier otra información clasificada o restringida, conforme a lo dispuesto en el ordenamiento jurídico costarricense.

El incumplimiento de esta disposición podrá generar responsabilidades administrativas, civiles o penales según corresponda.

12. CAPACITACIÓN Y SENSIBILIZACIÓN

La institución promoverá programas de capacitación y alfabetización digital sobre IA, fomentando el uso ético, seguro y responsable de estas tecnologías.

La participación en actividades formativas relacionadas con IA podrá ser obligatoria cuando así lo determine la Administración.

13. USO INDEBIDO DE LA IA

• Utilizar sistemas de inteligencia artificial para actividades ilícitas, fraudulentas o contrarias a los principios éticos y valores institucionales.

• Generar, difundir o utilizar información falsa, engañosa, manipulada o que induzca a error de forma deliberada.

• Compartir información confidencial, restringida o protegida en plataformas o servicios no autorizados por la Institución.

• Utilizar sistemas de inteligencia artificial para discriminar, acosar, vulnerar derechos fundamentales, afectar la dignidad humana o generar resultados que contravengan el ordenamiento jurídico vigente.

• Adoptar decisiones administrativas que produzcan efectos jurídicos o impacten significativamente los derechos, obligaciones o intereses de las personas cuando se basen

exclusivamente en procesos automatizados de inteligencia artificial y no cuenten con supervisión humana significativa o efectiva.

• La supervisión humana deberá permitir la revisión, validación, modificación o rechazo de las recomendaciones o resultados generados por el sistema de inteligencia artificial, garantizando el debido proceso administrativo y la rendición de cuentas correspondiente.

• Utilizar herramientas de inteligencia artificial no autorizadas por la Institución para procesar información institucional sensible, confidencial o protegida.

• El uso de sistemas de inteligencia artificial no exime el personal de la institución de su responsabilidad sobre las decisiones, actuaciones o productos generados con apoyo de dichas tecnologías.

14. INCIDENTES Y REPORTES

Será deber de todos los funcionarios / funcionarias sujetas a la presente política reportar de forma inmediata cualquier incidente, evento adverso o irregularidad relacionada con el uso de sistemas de inteligencia artificial, incluyendo, pero no limitado a:

• Fuga o exposición no autorizada de información.
• Uso indebido de herramientas de IA.
• Detección de sesgos, errores críticos o comportamientos anómalos.
• Vulnerabilidades de seguridad.
• Afectaciones operativas o institucionales derivadas del uso de IA.

El reporte deberá realizarse a la Unidad de Tecnologías de Información y Comunicación (UTIC), con copia a la jefatura inmediata, a través del canal oficial definido por la Institución para la gestión de incidentes tecnológicos. Dicho canal deberá garantizar trazabilidad, registro y seguimiento de cada caso.

Los incidentes deberán reportarse en los siguientes plazos:

• Incidentes críticos o de alto impacto: de forma inmediata o dentro de las primeras 2 horas desde su detección.
• Incidentes de impacto medio: dentro de las primeras 24 horas.
• Incidentes de bajo impacto: dentro de un plazo máximo de 72 horas.

La UTIC será responsable de clasificar el nivel de severidad del incidente, coordinar la respuesta técnica correspondiente y definir las acciones de contención, corrección y mitigación.

Cuando corresponda, la UTIC podrá escalar los incidentes a instancias externas competentes, tales como el Centro de Respuesta de Incidentes de Seguridad Informática de Costa Rica (CSIRT-CR), así como a la autoridad nacional competente en materia de protección de datos personales, de conformidad con la normativa vigente.

15. GUÍA INSTITUCIONAL PARA EL USO RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL

La institución dispone de una Guía Institucional para el Uso Responsable de la Inteligencia Artificial (IA) como documento complementario a la presente política, con el propósito de orientar a las personas funcionarias sobre las buenas prácticas, recomendaciones de uso, medidas de seguridad, ejemplos de aplicación y consideraciones para el uso adecuado de herramientas de Inteligencia Artificial en el ejercicio de sus funciones.

La guía podrá ser actualizada periódicamente por la Unidad de Tecnologías de Información y Comunicación (UTIC), conforme a la evolución tecnológica, las necesidades institucionales y las disposiciones normativas vigentes.

16. CUMPLIMIENTO

El incumplimiento de esta política podrá generar responsabilidades administrativas, civiles o penales conforme a la normativa vigente y el régimen disciplinario institucional.

17. VIGENCIA Y ACTUALIZACIÓN

La presente política entrará en vigor a partir de su aprobación oficial.
La UTIC realizará revisiones periódicas para asegurar su alineación con:

- Avances tecnológicos,
- Normativa nacional,
- Lineamientos del MICITT,
- Estrategia Nacional de IA,
- Mejores prácticas internacionales.

18. FIRMAS

Aprobación
JORGE MARIO RODRIGUEZ ZUÑIGA (FIRMA) Firmado digitalmente por JORGE MARIO RODRIGUEZ ZUÑIGA (FIRMA) Fecha: 2026.08.11 13:39:18 -06'00'

19. HISTORIAL DE VERSIONES

Versión	Fecha	Descripción de los cambios	Autor
1.0	27/05/2026	Creación del documento.	UTIC
1.1	04/06/2026	Ajustes varios en redacción y formato	Legal
1.2	06/06/2026	Redefinición de conceptos	UTIC
1.3	15/06/2026	Observaciones del MICITT	MICITT