FUNDAMEDIOS

RESUMEN PÚBLICO · 2026

Manual de Adopción y Uso de Inteligencia Artificial



La IA apoya, la responsabilidad es humana.

ECUADOR Chequea PERIODISMO CON RIGOR

Liberties 360°

Ilustración generada con IA

FUNDAMEDIOS

RESUMEN PÚBLICO · 2026

Manual de Adopción y Uso de Inteligencia Artificial

01 Presentación, objeto y ámbito de aplicación 03

02 Principios, riesgos, roles y reglas esenciales 05

03 Investigación, levantamiento y verificación de información con apoyo de IA 08

04 Gestión, protección y conservación de la información 12

05 Uso de inteligencia artificial para análisis, elaboración y publicación de contenidos 16

06 Gobernanza institucional, administración de herramientas y ciberseguridad 20

07 Cumplimiento, responsabilidad institucional y disposiciones finales 24



01

Presentación, objeto y ámbito de aplicación



La inteligencia artificial se ha incorporado como una herramienta de apoyo para la búsqueda, procesamiento, análisis y producción de información. Su utilización puede fortalecer las actividades periodísticas, investigativas, de verificación, monitoreo, comunicación y gestión desarrolladas por Fundamedios, Ecuador Chequea, Liberties 360° y sus demás proyectos, al facilitar tareas como el análisis documental, sistematización de información, identificación de patrones, elaboración de resúmenes y generación de borradores.

Sin embargo, su utilización también plantea riesgos relacionados con la exactitud de la información, generación de contenido falso o incorrecto, sesgos, protección de datos personales, confidencialidad, propiedad intelectual, seguridad de la información y determinación de responsabilidades. Por esta razón, Fundamedios adopta el presente Manual como marco institucional para incorporar herramientas de inteligencia artificial sin reducir sus estándares profesionales, periodísticos, investigativos, editoriales, éticos y de seguridad.

REGLA FUNDAMENTAL

La inteligencia artificial constituye una herramienta de asistencia y no sustituye el criterio profesional ni la responsabilidad humana.

Toda persona que investigue, verifique, analice, redacte, revise o autorice contenidos continuará siendo responsable de las decisiones adoptadas dentro de sus funciones. En consecuencia, las decisiones sustantivas y la publicación de contenidos deberán permanecer bajo control humano.

1.1. Objeto

El Manual establece los criterios, procedimientos y controles institucionales aplicables al uso de herramientas y sistemas de inteligencia artificial en las actividades de Fundamedios. Su finalidad es asegurar que la IA se utilice de manera responsable durante todo el ciclo de tratamiento y producción de información:

planificación → levantamiento de información → registro → clasificación → protección → verificación → análisis → producción → revisión humana → aprobación → publicación → conservación

Este procedimiento se sustenta en los siguientes principios:

exactitud y verificabilidad **transparencia y trazabilidad** **supervisión humana**
protección de datos personales y confidencialidad **seguridad de la información** **responsabilidad**
respeto de los estándares periodísticos y editoriales **cumplimiento de la normativa aplicable**

La trazabilidad deberá permitir que, ante errores, incidentes, reclamaciones o controversias, sea posible reconstruir el procedimiento seguido, identificar las fuentes utilizadas, determinar los controles aplicados y establecer las responsabilidades correspondientes.

1.2. Ámbito de aplicación

El Manual será aplicable a todas las actividades desarrolladas por Fundamedios, Ecuador Chequea, Liberties 360° y cualquier otro proyecto, programa, plataforma o iniciativa administrada por la organización.

Sus disposiciones deberán ser observadas por directivos, periodistas, editores, investigadores, verificadores, analistas, personal técnico y administrativo, consultores, colaboradores, pasantes y, cuando corresponda, proveedores o terceros que procesen información por cuenta de Fundamedios. También se aplicarán tanto a herramientas contratadas institucionalmente como a aquellas utilizadas individualmente para desarrollar actividades o productos destinados a la organización.

Comprende, entre otros, el uso de IA para investigación, búsqueda y levantamiento de información, monitoreo, verificación, análisis documental y de datos, clasificación, transcripción, traducción, elaboración de resúmenes, generación y edición de textos, producción audiovisual y preparación de alertas, notas e informes.

1.3. Estructura operativa

El Manual organiza el uso institucional de inteligencia artificial alrededor de dos grandes etapas:

a)

Obtención y tratamiento de información

Búsqueda, recolección, clasificación, almacenamiento, protección, análisis y verificación.

b)

Producción y publicación

Utilización de información previamente validada para elaborar alertas, verificaciones, notas, informes, contenidos digitales y demás productos institucionales.

Entre ambas etapas deberá existir siempre una verificación y supervisión humana proporcional a la naturaleza y nivel de riesgo de la información. Los procedimientos posteriores desarrollan los controles necesarios para que cada utilización de IA pueda ser documentada, revisada y, cuando sea necesario, auditada.



REGLA TRANSVERSAL

La IA puede asistir el proceso; la responsabilidad, verificación y decisión final permanecen en las personas.

02

Principios, riesgos, roles y reglas esenciales



2.1. Principios fundamentales para el uso de IA

Toda utilización de herramientas de inteligencia artificial deberá observar los siguientes principios:

a) Exactitud y verificabilidad

La información generada, procesada o sugerida por una herramienta de IA no puede asumirse como verdadera únicamente por provenir del sistema. La IA puede producir errores, datos inexistentes, referencias incorrectas o interpretaciones equivocadas; por ello, todo contenido relevante deberá ser contrastado con fuentes confiables antes de ser utilizado.

> **La respuesta generada por una IA no constituye una fuente de información por sí misma.**

b) Trazabilidad

Todo proceso que utilice inteligencia artificial debe permitir reconstruir qué herramienta fue utilizada, qué información se proporcionó, qué resultado generó, qué verificaciones se realizaron y quién tomó la decisión final.

La trazabilidad permite identificar fallas, corregir errores y determinar responsabilidades cuando existan reclamos, incidentes o controversias.

c) Supervisión humana

La inteligencia artificial no reemplaza el análisis profesional, la revisión editorial ni la toma de decisiones institucionales. La persona responsable del producto conserva la obligación de evaluar la pertinencia, exactitud, riesgos y consecuencias del resultado obtenido.

d) Protección de información

El uso de IA deberá respetar las reglas institucionales sobre datos personales, información confidencial, fuentes protegidas, investigaciones en curso y seguridad digital. La facilidad de procesamiento que ofrecen estas herramientas no elimina las obligaciones de protección sobre la información entregada.

e) Responsabilidad

La utilización de IA no traslada la responsabilidad a la herramienta tecnológica. Las decisiones sobre investigación, publicación, análisis o difusión continúan correspondiendo a las personas responsables dentro de la organización.

2.2. Clasificación de riesgos en el uso de IA

Para determinar el nivel de control requerido, el Manual establece una clasificación según el impacto potencial del uso de inteligencia artificial.

Bajo — **Crítico**

RIESGO BAJO

Comprende actividades internas o de apoyo que no involucran información sensible ni generan directamente productos públicos. Ejemplos:

- organización de ideas;
- generación de esquemas;
- elaboración de borradores iniciales;
- apoyo administrativo.

Aunque requieren revisión, no generan un impacto significativo si presentan errores.

RIESGO MEDIO

Incluye usos que pueden influir en productos institucionales o análisis internos, pero que cuentan con mecanismos posteriores de revisión. Ejemplos:

- resúmenes de documentos;
- apoyo en análisis preliminares;
- clasificación de información;
- procesamiento de datos no sensibles.

Requieren validación humana antes de su utilización.

RIESGO ALTO

Comprende actividades relacionadas con información sensible, investigaciones, contenidos públicos o decisiones que pueden afectar derechos, reputación o seguridad institucional. Ejemplos:

- análisis de investigaciones periodísticas;
- procesamiento de documentos confidenciales;
- elaboración de contenidos que serán publicados;
- tratamiento de información de fuentes protegidas.

Exige controles reforzados, revisión especializada y trazabilidad completa.

RIESGO CRÍTICO

Corresponde a usos cuyo error podría generar afectaciones graves a personas, fuentes, investigaciones o a la organización. Incluye, entre otros:

- procesamiento de información altamente confidencial sin autorización;
- generación de contenidos que puedan atribuir falsamente hechos a personas;
- decisiones automatizadas sin revisión humana;
- exposición de información protegida.

Estos usos requieren autorización expresa o pueden encontrarse prohibidos según la naturaleza del caso.

2.3. Roles y responsabilidades institucionales

El Manual distribuye responsabilidades para evitar que el uso de IA quede sin control definido.



Operador de IA

Es la persona que utiliza directamente la herramienta. Tiene la obligación de:

- utilizar herramientas autorizadas;
- proteger la información ingresada;
- documentar usos relevantes;
- revisar críticamente los resultados generados.



Responsable del producto

Es quien responde por el contenido final, investigación o resultado en el que intervino la IA. Debe garantizar que la información sea adecuada, verificable y cumpla los estándares institucionales.



Revisor humano

Realiza la evaluación independiente del resultado generado, especialmente en usos de riesgo medio, alto o crítico. Su función es detectar errores, inconsistencias, sesgos o riesgos antes de la aprobación.



Aprobador editorial o institucional

Cuando corresponda, autoriza la publicación o utilización definitiva del producto, verificando que se hayan cumplido los controles establecidos.

2.4. Reglas esenciales para la utilización de herramientas de IA

Para garantizar un uso seguro, Fundamedios establece las siguientes reglas generales:

1
Utilizar únicamente herramientas autorizadas por la organización.

2
No ingresar información confidencial, datos personales sensibles, información de fuentes protegidas o investigaciones no publicadas en herramientas no aprobadas.

3
No utilizar resultados generados por IA sin verificación humana previa cuando puedan afectar la calidad, reputación o derechos de terceros.

4
Mantener registros suficientes cuando el uso de IA sea relevante para un producto institucional.

5
No atribuir a la IA decisiones editoriales, jurídicas, investigativas o institucionales.

6
Aplicar controles adicionales cuando aumente la sensibilidad de la información o el impacto potencial del resultado.

03

Investigación, levantamiento y verificación de información con apoyo de IA



La inteligencia artificial puede convertirse en una herramienta útil para fortalecer los procesos de investigación mediante la búsqueda, organización, análisis y sistematización de información. Sin embargo, su utilización dentro de procesos periodísticos, investigativos o de verificación exige controles estrictos, debido a que los sistemas de IA pueden generar información incorrecta, incompleta, descontextualizada o inexistente.

Por esta razón, Fundamedios establece que la IA puede apoyar la investigación, pero no reemplaza las etapas esenciales de búsqueda, contraste, análisis y verificación profesional. Toda información obtenida mediante herramientas de IA deberá pasar por un proceso de validación antes de ser incorporada a productos institucionales.

El ciclo general de investigación deberá seguir la siguiente lógica:

Planificación → **búsqueda y recopilación** → **evaluación de fuentes** → **verificación** → **organización de información** → **análisis** → **producción**

3.1. Planificación de la investigación

Antes de utilizar herramientas de inteligencia artificial, el equipo deberá definir con claridad:

- cuál es la pregunta o problema de investigación;
- cuál es la información que se busca obtener;
- cuál es la finalidad del análisis;
- qué fuentes serán necesarias;
- qué riesgos pueden existir en el tratamiento de la información.

La IA no debe utilizarse como sustituto de una investigación previamente estructurada. Un uso inadecuado puede generar búsquedas amplias, sesgadas o basadas en información no comprobada.

Por ello, antes de ingresar una consulta a una herramienta de IA debe existir una definición clara del objetivo investigativo.

3.2. Uso de IA para búsqueda y levantamiento de información

La inteligencia artificial puede emplearse como herramienta auxiliar para:

- identificar posibles líneas de investigación;
- organizar grandes volúmenes de información;
- resumir documentos previamente obtenidos;
- generar preguntas de investigación;
- detectar relaciones o patrones preliminares;
- facilitar la revisión inicial de materiales.

No obstante, los resultados obtenidos mediante IA deberán considerarse únicamente como insumos exploratorios.

La IA no reemplaza la consulta de fuentes originales ni permite asumir como ciertos los datos proporcionados por el sistema.

Toda información relevante deberá regresar a la fuente primaria o secundaria correspondiente para confirmar:



- existencia del documento
- autenticidad
- fecha
- autoría
- contexto
- interpretación correcta

3.3. Evaluación y selección de fuentes

La calidad de una investigación depende principalmente de la calidad de sus fuentes. Por ello, la información identificada con apoyo de IA deberá evaluarse considerando:

Autoridad de la fuente

Debe determinarse quién genera la información, cuál es su competencia sobre el tema y si existe un interés particular que pueda afectar su imparcialidad.

Fiabilidad

Debe verificarse si la información cuenta con respaldo documental, evidencia comprobable o antecedentes consistentes.

Actualidad

Debe analizarse si la información corresponde al período investigado y si continúa siendo válida.

Contexto

Debe evitarse utilizar fragmentos aislados que puedan modificar el sentido original de una declaración, documento o dato.

3.4. Verificación obligatoria de información generada o encontrada mediante IA

Toda información obtenida con apoyo de inteligencia artificial deberá ser verificada antes de utilizarse en:

- investigaciones;
- verificaciones de datos;
- informes;
- publicaciones;
- alertas;
- análisis institucionales.

La verificación deberá incluir, según corresponda:

- revisión de fuentes originales;
- contraste con fuentes independientes;
- comprobación documental;
- validación de citas;
- confirmación de cifras y fechas;
- revisión del contexto completo.

REGLA INSTITUCIONAL

La IA puede ayudar a encontrar información; únicamente la verificación humana puede convertirla en información utilizable.

3.5. Control de sesgos y errores

Las herramientas de IA pueden reproducir errores presentes en los datos con los que fueron entrenadas o generar respuestas influenciadas por la forma en que se formula una consulta.

Para reducir estos riesgos, quienes utilicen IA deberán:

- formular preguntas neutrales;
- evitar búsquedas orientadas únicamente a confirmar una hipótesis previa;
- revisar respuestas alternativas;
- identificar información faltante;
- cuestionar afirmaciones que no tengan respaldo verificable.

> **La investigación debe orientarse a comprobar hechos, no a confirmar conclusiones previamente establecidas.**

3.6. Clasificación del estado de la información

Durante el proceso investigativo, la información deberá diferenciarse según su nivel de validación:

1

Información exploratoria

Datos obtenidos durante una búsqueda inicial o mediante herramientas de IA que requieren comprobación.

2

Información pendiente de verificación

Elementos que pueden ser útiles para la investigación, pero cuya autenticidad o precisión todavía no ha sido confirmada.

3

Información parcialmente verificada

Datos que cuentan con algunos elementos comprobados, pero requieren mayor contraste.

4

Información validada

Información comprobada mediante fuentes confiables y suficiente evidencia documental.

Solo la información validada deberá incorporarse como fundamento de productos institucionales.

3.7. Registro y trazabilidad del proceso investigativo



Cuando el uso de IA sea relevante dentro de una investigación, deberá conservarse información suficiente para reconstruir el proceso:

- herramienta utilizada;
- finalidad del uso;
- tipo de información proporcionada;
- resultados obtenidos;
- verificaciones realizadas;
- persona responsable.

Esto permite garantizar transparencia, corregir errores y evaluar posteriormente la metodología aplicada.

04

Gestión, protección y conservación de la información



La gestión adecuada de la información constituye uno de los elementos esenciales para el uso responsable de inteligencia artificial dentro de Fundamedios. La incorporación de herramientas tecnológicas no modifica las obligaciones institucionales relacionadas con la confidencialidad, protección de datos, seguridad de la información y resguardo de fuentes.

La información debe ser protegida durante todo su ciclo de vida, desde su recopilación hasta su eliminación o archivo definitivo. El uso de IA aumenta la necesidad de aplicar controles, debido a que los sistemas pueden requerir el ingreso temporal de información para su procesamiento, generando riesgos relacionados con exposición, almacenamiento, reutilización o acceso no autorizado.

REGLA INSTITUCIONAL

La información utilizada con herramientas de inteligencia artificial conserva la misma clasificación, sensibilidad y obligaciones de protección que tendría fuera de dichos sistemas.

4.1. Ciclo de vida de la información

Toda información institucional deberá gestionarse bajo un ciclo ordenado:

Obtención → **clasificación** → **almacenamiento** → **uso** → **conservación** → **eliminación o archivo**

Cada etapa requiere medidas de control adecuadas según la naturaleza de la información y los riesgos asociados.

La utilización de IA no debe romper este ciclo ni generar tratamientos informales de información fuera de los mecanismos institucionales establecidos.

4.2. Clasificación de la información

Antes de utilizar información en una herramienta de inteligencia artificial, deberá determinarse su nivel de sensibilidad.

PÚBLICA

Corresponde a aquella información autorizada para difusión o que ya se encuentra disponible públicamente.

Puede utilizarse en herramientas autorizadas siempre que no existan riesgos adicionales.

INTERNA

Comprende información de trabajo institucional que no está destinada a difusión pública, pero cuyo acceso está permitido dentro de la organización.

Su utilización deberá limitarse al personal autorizado y a herramientas aprobadas.

CONFIDENCIAL

Incluye información cuya divulgación podría afectar investigaciones, proyectos, relaciones institucionales o intereses legítimos de la organización.

Su tratamiento requiere controles reforzados y autorización según corresponda.

RESTRINGIDA

Comprende información de mayor sensibilidad, como:

- datos personales protegidos;
- información de fuentes confidenciales;
- investigaciones no publicadas;
- información cuya exposición pueda generar daños relevantes.

No deberá ingresarse en herramientas no autorizadas o sin garantías suficientes de seguridad.

4.3. Protección de datos personales

El uso de inteligencia artificial deberá respetar los principios aplicables al tratamiento de datos personales, especialmente:

finalidad determinada | **minimización** | **proporcionalidad** | **seguridad** | **confidencialidad**

Antes de ingresar datos personales a una herramienta de IA deberá evaluarse:

- si la información es necesaria para la finalidad perseguida;
- si puede utilizarse información anonimizada o reducida;
- si existe autorización para su tratamiento;
- si la herramienta ofrece condiciones adecuadas de protección.

> **La disponibilidad tecnológica de una herramienta no constituye autorización automática para ingresar información personal.**

4.4. Fuentes confidenciales e información protegida



La protección de fuentes constituye un elemento esencial del trabajo periodístico e investigativo.

En consecuencia:

- no deberán incorporarse datos que permitan identificar fuentes protegidas en herramientas no autorizadas;
- deberán aplicarse medidas de anonimización cuando sea posible;
- la información entregada por fuentes confidenciales deberá mantenerse bajo controles estrictos;
- cualquier uso de IA que pueda comprometer una fuente deberá ser evaluado previamente.

La utilización de inteligencia artificial nunca debe convertirse en un mecanismo que exponga información cuya protección resulta esencial para la actividad institucional.

4.5. Investigaciones en curso y documentos no publicados

La información correspondiente a investigaciones abiertas, borradores internos, documentos preliminares, bases de datos de trabajo o contenidos pendientes de publicación requiere un nivel elevado de protección.

Antes de utilizar este tipo de información con IA deberá analizarse:

- el nivel de confidencialidad;
- el riesgo de exposición;
- la necesidad real de utilizar la herramienta;
- la existencia de alternativas más seguras.

Cuando sea posible, deberá emplearse información reducida, anonimizada o fragmentada, evitando entregar a sistemas externos conjuntos completos de información sensible.

4.6. Almacenamiento, acceso y conservación

La información generada o procesada con apoyo de IA deberá conservarse conforme a los mecanismos institucionales definidos.

Deberán establecerse controles sobre:



- quién puede acceder a la información;
- dónde se almacena;
- cuánto tiempo debe conservarse;
- qué usuarios tienen permisos;
- cuándo corresponde su eliminación.

El acceso deberá responder al principio de necesidad de conocer, es decir, únicamente tendrán acceso quienes requieran la información para cumplir sus funciones.

4.7. Eliminación segura de información

Cuando la información ya no sea necesaria para la finalidad que justificó su tratamiento, deberá aplicarse un proceso de eliminación segura conforme a las políticas institucionales.

La eliminación deberá considerar:

archivos originales | copias de trabajo | documentos derivados | registros utilizados durante procesos de IA

No debe asumirse que eliminar un archivo local elimina automáticamente toda información procesada por una herramienta externa; por ello, la selección de plataformas y la revisión de sus condiciones de almacenamiento resulta fundamental.

4.8. Reglas prácticas para el uso seguro de información con IA

ANTES DE INGRESAR INFORMACIÓN A UNA HERRAMIENTA DE INTELIGENCIA ARTIFICIAL, LA PERSONA USUARIA DEBERÁ PREGUNTARSE:

1. **¿Tengo autorización para utilizar esta información?**
2. **¿La herramienta está aprobada institucionalmente?**
3. **¿La información contiene datos personales, fuentes protegidas o información confidencial?**
4. **¿Puedo reducir, anonimizar o reemplazar la información?**
5. **¿Puedo justificar posteriormente por qué utilicé esta herramienta?**

Si alguna respuesta genera dudas, deberá detenerse el proceso y solicitar orientación.

05

Uso de inteligencia artificial para análisis, elaboración y publicación de contenidos



La inteligencia artificial puede contribuir a mejorar los procesos de análisis, redacción, edición y producción de contenidos institucionales. Sin embargo, su incorporación dentro de actividades periodísticas y comunicacionales debe mantener los estándares de precisión, independencia editorial, transparencia y responsabilidad profesional.

La IA puede asistir en tareas operativas y creativas, pero no puede sustituir la investigación, el criterio periodístico, la revisión editorial ni la decisión humana sobre la publicación de un contenido.

REGLA FUNDAMENTAL DE ESTE CAPÍTULO

La inteligencia artificial puede participar en la elaboración de un contenido, pero la responsabilidad sobre lo publicado siempre corresponde a las personas responsables del producto.

5.1. Preparación del uso de IA para producción de contenidos

Antes de utilizar una herramienta de inteligencia artificial para elaborar un contenido, deberá definirse:

- cuál es el producto que se busca generar;
- cuál es la información base que será utilizada;
- cuál es el público destinatario;
- qué riesgos puede generar el resultado;
- qué nivel de revisión será necesario.

El uso de IA debe realizarse sobre información previamente analizada y validada. No debe utilizarse como mecanismo para generar contenidos basados únicamente en información no comprobada.

La calidad del resultado depende directamente de la calidad del material proporcionado a la herramienta.

5.2. Elaboración de textos y productos institucionales

La IA puede utilizarse como apoyo para:

- estructurar documentos;
- mejorar redacción;
- generar esquemas iniciales;
- resumir información previamente validada;
- adaptar contenidos a diferentes formatos;
- proponer títulos o enfoques comunicacionales.

Sin embargo, los textos generados deberán ser revisados antes de cualquier uso institucional. La revisión deberá verificar:

- exactitud de datos;
- coherencia del contenido;
- correcta atribución de declaraciones;
- ausencia de afirmaciones inventadas;
- eliminación de errores generados por la herramienta;
- adecuación al estilo institucional.

> **Un texto generado automáticamente no equivale a un contenido terminado.**

5.3. Prohibición de generación de información falsa o no comprobada

Las herramientas de IA pueden producir respuestas incorrectas mediante mecanismos conocidos como “alucinaciones”, en los cuales generan información aparentemente válida pero inexistente.

Por ello, está prohibido utilizar IA para:

- ✕ inventar datos;
- ✕ crear fuentes inexistentes;
- ✕ atribuir declaraciones falsas a personas;
- ✕ fabricar citas;
- ✕ completar vacíos de información mediante suposiciones;
- ✕ presentar como hechos afirmaciones no verificadas.

Cuando una herramienta no tenga información suficiente, la respuesta adecuada es continuar la investigación, no completar artificialmente la información faltante.

5.4. Citas, datos y atribuciones

Toda cita, cifra, referencia normativa, documento, declaración pública o dato utilizado en un producto institucional deberá ser comprobado.

Cuando un contenido incluya:

declaraciones de personas · **datos estadísticos** · **documentos oficiales** · **referencias legales** · **información histórica**

deberá verificarse su existencia y contexto antes de su publicación.

La IA puede ayudar a localizar o procesar información, pero no puede ser considerada una fuente de autoridad para respaldar afirmaciones.

5.5. Revisión humana y aprobación editorial

Todo contenido elaborado con apoyo de inteligencia artificial deberá pasar por controles humanos proporcionales al nivel de riesgo.

La revisión deberá considerar:



Revisión factual

Determina si los hechos, cifras, nombres, fechas y referencias son correctos.



Revisión contextual

Evalúa si la información mantiene el sentido original y evita interpretaciones equivocadas.



Revisión editorial

Verifica claridad, coherencia, enfoque institucional y cumplimiento de estándares comunicacionales.



Revisión ética y de riesgos

Analiza posibles afectaciones a personas, fuentes, grupos vulnerables o reputación institucional.

La publicación solo podrá realizarse cuando estos controles hayan sido cumplidos.

5.6. Transparencia sobre el uso de IA

Cuando el uso de inteligencia artificial sea relevante para la elaboración de un contenido, Fundamedios deberá evaluar si corresponde informar esta circunstancia.

La transparencia busca mantener la confianza de las audiencias y permitir distinguir entre:

Contenidos completamente elaborados por personas

Contenidos elaborados con asistencia tecnológica

Contenidos generados sintéticamente

La comunicación sobre el uso de IA deberá realizarse considerando la naturaleza del producto y el posible impacto en la audiencia.

5.7. Uso de IA en imágenes, audio y video

Los contenidos audiovisuales generados o modificados mediante IA requieren controles adicionales debido a la posibilidad de crear representaciones falsas o engañosas.

Antes de publicar materiales sintéticos deberá verificarse:

- si existe una persona real representada;
- si la modificación puede inducir a error;
- si se afecta la reputación o derechos de terceros;
- si debe incorporarse una advertencia o identificación del uso de IA.

Está prohibido utilizar contenido generado artificialmente de manera que pueda confundirse con material auténtico cuando ello pueda afectar la comprensión de la audiencia.

5.8. Archivo y trazabilidad del contenido generado con IA

Cuando un producto institucional haya utilizado inteligencia artificial de manera significativa, deberá conservarse información suficiente para reconstruir el proceso:

- herramienta utilizada;
- finalidad del uso;
- información proporcionada;
- modificaciones realizadas;
- revisiones efectuadas;
- responsables de aprobación.

Esto permite mantener transparencia interna y responder adecuadamente ante errores o cuestionamientos posteriores.

5.9. Flujo operativo para publicación de contenidos con IA

El proceso institucional deberá seguir esta secuencia:

01	Información validada
02	Asistencia de IA
03	Revisión humana
04	Verificación factual
05	Revisión editorial
06	Aprobación
07	Publicación



ANTES DE PUBLICAR

Ningún resultado generado por IA deberá pasar directamente a publicación sin revisión humana.

06

Gobernanza institucional, administración de herramientas y ciberseguridad



La incorporación de inteligencia artificial dentro de Fundamedios requiere no solo reglas sobre el uso individual de herramientas, sino también un modelo institucional que permita administrar accesos, controlar riesgos, proteger información y responder adecuadamente frente a incidentes.

La gobernanza de IA tiene como finalidad asegurar que las herramientas utilizadas por la organización sean conocidas, evaluadas, administradas y utilizadas bajo criterios uniformes de seguridad, eficiencia y responsabilidad.

REGLA CENTRAL DE ESTE CAPÍTULO

La inteligencia artificial debe gestionarse como un recurso institucional sujeto a controles de seguridad, no como una herramienta personal sin supervisión.

6.1. Administración institucional de herramientas de IA

Fundamedios deberá mantener un control sobre las herramientas de inteligencia artificial utilizadas dentro de sus actividades institucionales.

Este control deberá permitir identificar:

- qué herramientas están autorizadas;
- para qué finalidades pueden utilizarse;
- qué usuarios tienen acceso;
- qué información puede procesarse;
- cuáles son sus riesgos y limitaciones.

La selección de herramientas deberá considerar aspectos como:

- seguridad de la información;
- condiciones de almacenamiento;
- tratamiento de datos ingresados;
- disponibilidad de controles administrativos;
- cumplimiento de estándares institucionales.

No deberá utilizarse una herramienta únicamente por su disponibilidad o popularidad, sino por su adecuación a las necesidades y riesgos de la organización.

6.2. Gestión de usuarios y permisos

El acceso a herramientas institucionales deberá administrarse bajo criterios de necesidad y proporcionalidad.

Los permisos deberán asignarse considerando:

funciones del usuario **tipo de información que puede procesar**

nivel de riesgo de las actividades realizadas

Cada usuario deberá contar únicamente con los accesos necesarios para cumplir sus responsabilidades.

La organización deberá implementar medidas como:

- creación y eliminación oportuna de usuarios;
- revisión periódica de permisos;
- retiro de accesos cuando finalice una relación laboral o contractual;
- protección de credenciales.



El uso compartido de cuentas personales o institucionales deberá evitarse cuando impida identificar quién realizó una acción determinada.

6.3. Capacitación y cultura institucional

El uso seguro de inteligencia artificial depende de que las personas conozcan sus capacidades, limitaciones y riesgos.

Por ello, Fundamedios deberá promover procesos de capacitación orientados a:

uso responsable de herramientas **identificación de errores generados por IA**

protección de información **verificación de resultados** **prevención de riesgos de seguridad**

> **La capacitación no debe enfocarse únicamente en aprender a utilizar herramientas, sino en comprender cuándo no deben utilizarse.**

6.4. Seguridad de la información en entornos de IA

Las herramientas de inteligencia artificial pueden generar riesgos relacionados con acceso indebido, filtración de información, manipulación de instrucciones o exposición de datos.

Para reducir estos riesgos deberán aplicarse medidas como:

- utilización de cuentas institucionales cuando corresponda;
- autenticación segura;
- contraseñas robustas;
- control de accesos;
- actualización de herramientas;
- revisión de configuraciones de privacidad.

La seguridad debe considerarse desde el momento en que se selecciona una herramienta, no únicamente cuando ocurre un incidente.

6.5. Riesgos específicos de seguridad asociados a IA

El uso de inteligencia artificial introduce riesgos particulares que requieren atención institucional.

a) Ingreso indebido de información

Puede ocurrir cuando usuarios incorporan datos confidenciales, personales o sensibles en herramientas que no cuentan con autorización.

Medida preventiva:

- clasificación previa de la información;
- capacitación;
- controles sobre herramientas autorizadas.

b) Manipulación de instrucciones (prompt injection)

Consiste en intentos de modificar el comportamiento de un sistema mediante instrucciones diseñadas para evadir controles o revelar información protegida.

Medidas preventivas:

- evitar ingresar información sensible en sistemas no confiables;
- revisar resultados generados;
- limitar permisos.

c) Generación de contenido falso

La IA puede producir información incorrecta con apariencia de precisión.

Medida preventiva:

- verificación humana;
- contraste con fuentes;
- prohibición de utilizar resultados sin revisión.

d) Dependencia tecnológica

Un uso excesivo de IA puede generar pérdida de criterio profesional o aceptación automática de resultados.

Medida preventiva:

- mantener capacidades humanas de análisis;
- utilizar IA como apoyo, no como sustituto del conocimiento institucional.

6.6. Gestión de incidentes relacionados con IA

Un incidente relacionado con inteligencia artificial puede incluir:

- exposición accidental de información;
- uso no autorizado de herramientas;
- generación o publicación de información incorrecta;
- pérdida de trazabilidad;
- acceso indebido a sistemas.

Ante un incidente deberá:

1. identificarse la situación
2. contenerse el riesgo
3. preservar evidencia relevante
4. informar a los responsables correspondientes
5. evaluar impactos
6. aplicar medidas correctivas

La respuesta deberá orientarse no solo a corregir el problema inmediato, sino también a evitar su repetición.

6.7. Continuidad operativa y recuperación

Fundamedios deberá considerar escenarios en los cuales una herramienta de IA deje de estar disponible, cambie sus condiciones de servicio o presente fallas.

Por ello, los procesos institucionales no deberán depender exclusivamente de una herramienta tecnológica específica.

Deberán mantenerse:

procedimientos alternativos **respaldo de información** **documentación de procesos**

capacidad humana para continuar las actividades esenciales

> **La IA debe fortalecer la operación institucional, pero nunca convertirse en un punto único de falla.**

6.8. Revisión periódica del modelo de gobernanza



Debido a la rápida evolución de las tecnologías de inteligencia artificial, las herramientas, riesgos y buenas prácticas deberán revisarse periódicamente.

La organización deberá evaluar:

- nuevas herramientas disponibles;
- cambios regulatorios;
- incidentes ocurridos;
- necesidades de capacitación;
- actualización de controles.

La gobernanza de IA debe entenderse como un proceso dinámico y no como una regla estática.

07

Cumplimiento, responsabilidad institucional y disposiciones finales



El uso de inteligencia artificial dentro de Fundamedios debe desarrollarse bajo un marco de responsabilidad institucional que garantice que las herramientas tecnológicas se utilicen de manera ética, segura y coherente con la misión de la organización.

La existencia de herramientas de IA no modifica las obligaciones profesionales, periodísticas, investigativas, administrativas o institucionales de quienes las utilizan. La tecnología puede asistir procesos, pero no elimina la obligación de actuar con diligencia, verificar información y proteger los derechos de terceros.

REGLA CENTRAL DE ESTE CAPÍTULO

El uso responsable de inteligencia artificial depende de las decisiones humanas, los controles institucionales y el cumplimiento permanente de las reglas establecidas.

7.1. Cumplimiento obligatorio del Manual

El presente Manual constituye el marco institucional para el uso de herramientas de inteligencia artificial dentro de Fundamedios y sus proyectos relacionados.

Sus disposiciones son aplicables a todas las personas que utilicen herramientas de IA en actividades institucionales, incluyendo:

personal permanente · **colaboradores** · **consultores** · **proveedores** · **investigadores** · **periodistas** · **equipos técnicos y administrativos**

El cumplimiento del Manual no depende del tipo de herramienta utilizada, sino de la actividad desarrollada y del tratamiento de información realizado.

7.2. Responsabilidad de las personas usuarias

Cada persona que utilice inteligencia artificial dentro de sus funciones deberá actuar conforme a los principios establecidos en este Manual.

Entre sus obligaciones se encuentran:

- utilizar herramientas autorizadas;
- proteger la información ingresada;
- verificar los resultados obtenidos;
- mantener trazabilidad cuando corresponda;

- informar riesgos o incidentes;
- cumplir los procesos internos de revisión y aprobación.

> **La persona usuaria no podrá justificar una actuación incorrecta alegando que el resultado fue generado por una herramienta de inteligencia artificial.**

7.3. Responsabilidad institucional

Fundamedios, como organización, tiene la responsabilidad de establecer las condiciones necesarias para un uso seguro y responsable de IA mediante:

- definición de políticas y procedimientos;
- autorización de herramientas;
- capacitación del personal;
- implementación de controles de seguridad;
- seguimiento de riesgos;
- actualización periódica del Manual.

La responsabilidad institucional no consiste únicamente en controlar errores, sino en crear un entorno donde el uso de IA pueda desarrollarse bajo criterios claros y previsibles.

7.4. Errores, incumplimientos y evaluación de responsabilidades

La generación de un error por parte de una herramienta de inteligencia artificial no determina automáticamente responsabilidad de la persona usuaria.

Para evaluar una situación deberá analizarse:

- la naturaleza del error;
- la información proporcionada a la herramienta;
- los controles aplicados;
- el nivel de revisión realizado;
- las obligaciones asignadas a cada persona involucrada.

De esta manera, deberá diferenciarse entre:

Error no intencional
Puede producirse pese a haber aplicado los controles razonables establecidos.

Falta de diligencia
Ocurre cuando no se aplicaron las verificaciones, revisiones o medidas de seguridad esperadas.

Incumplimiento deliberado
Se presenta cuando una persona omite conscientemente las reglas institucionales, utiliza herramientas prohibidas o expone información protegida.

7.5. Reporte y tratamiento de incumplimientos

Las personas integrantes de Fundamedios deberán informar situaciones que puedan representar riesgos relacionados con IA, tales como:

- uso de herramientas no autorizadas;
- exposición de información;
- publicación de contenido incorrecto generado mediante IA;

- pérdida de trazabilidad;
- incumplimiento de controles establecidos.

El reporte oportuno permite corregir errores, reducir impactos y fortalecer los mecanismos institucionales.

7.6. Actualización permanente del Manual

La inteligencia artificial es una tecnología en constante evolución. Por ello, este Manual deberá revisarse periódicamente para incorporar:

nuevos riesgos **cambios tecnológicos** **modificaciones regulatorias**
aprendizajes derivados de incidentes **nuevas necesidades institucionales**

Las actualizaciones deberán mantener el equilibrio entre innovación y protección de los estándares institucionales.

7.7. Integración con otras políticas institucionales

El uso de inteligencia artificial deberá interpretarse conjuntamente con las demás políticas y normas internas aplicables, especialmente aquellas relacionadas con:

- seguridad de información;
- protección de datos personales;
- ética institucional;
- tratamiento documental;
- estándares periodísticos;
- propiedad intelectual.

Cuando exista conflicto entre la utilización de una herramienta tecnológica y las obligaciones institucionales, deberán prevalecer los principios de protección, responsabilidad y cumplimiento normativo.

7.8. Cierre del modelo institucional de IA

El modelo adoptado por Fundamedios parte de una premisa fundamental: la inteligencia artificial representa una oportunidad para fortalecer procesos institucionales, pero su valor depende de la manera en que sea utilizada.

La organización busca promover un uso que combine:

innovación tecnológica **rigor profesional** **protección de derechos**
seguridad de la información **responsabilidad humana**

Por ello, la implementación de IA debe orientarse a mejorar capacidades institucionales sin afectar la confianza, independencia y calidad de los productos desarrollados por Fundamedios.



La IA apoya,
la responsabilidad es humana.

FUNDAMEDIOS · ECUADOR Chequea PERIODISMO CON RIGOR · Liberties 360°

José Padilla N 330 e Iñaquito, Edificio Platinum, piso 10, oficina 1002 · Quito, Ecuador · (593) 2 601 9956 · info@fundamedios.org · www.fundamedios.org

Ilustraciones e íconos generados con IA.