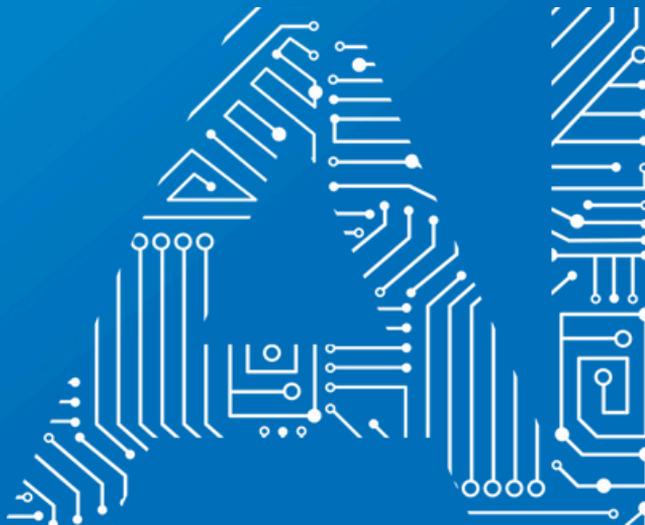


Código ético para el desarrollo, uso e implementación de Inteligencia Artificial en Euskadi

BAC BASQUE ARTIFICIAL
INTELLIGENCE
CENTER





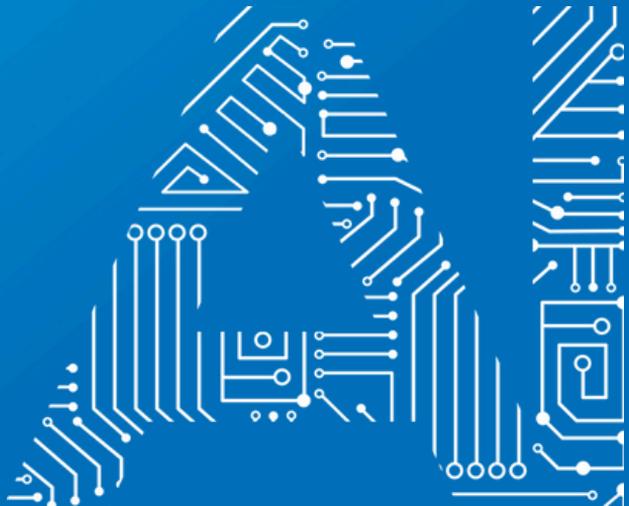
Contenido

- 1.Contexto
- 2.Consideraciones éticas fundamentales
- 3.Aplicación de los principios éticos en el uso, desarrollo e implementación de la IA.
4. Procesos para la implementación y actualización de este documento.
5. Recomendaciones y siguientes pasos

Código ético para el desarrollo, uso e implementación de Inteligencia Artificial en Euskadi

BAC

BASQUE ARTIFICIAL
INTELLIGENCE CENTER





Contexto

1.Contexto

1.1 Definición de IA

Existen distintas definiciones de Inteligencia Artificial (IA) que han sido utilizadas desde que, en 1956 John McCarthy, Marvin Minsky y Claude Shannon acuñaran el término en la conferencia de Dartmouth en la cual conjeturaban que cada aspecto de la inteligencia o del aprendizaje puede ser descrito tan precisamente que una máquina pueda simularlo. Estas definiciones reflejan el objetivo común de la IA, que es la creación de sistemas capaces de imitar o emular la inteligencia humana en diversas áreas de aplicación. La IA abarca una amplia gama de técnicas, como el aprendizaje automático (*machine learning*), la visión por computadora, el procesamiento del lenguaje natural y la robótica, entre otras. De cara a visibilizar nuestro compromiso y alineación con las políticas y directrices establecidas por la Unión Europea se tomará como base para este documento la definición incluida en el Reglamento de Inteligencia Artificial (RIA) en vigor desde el 1 de agosto de 2024 [<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>]:

Sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

1.2 Propósito del documento

El presente documento se genera como consecuencia de la responsabilidad adquirida por el ecosistema vasco de IA compuesto por administraciones públicas, empresas, agentes de conocimiento y centros científico-tecnológicos en el contexto del desarrollo, uso e implementación de la IA y establece un marco ético para el uso, implementación y desarrollo de la Inteligencia Artificial en el ecosistema de Euskadi. Su objetivo es promover prácticas éticas y responsables que maximicen los beneficios de la IA, aseguren su fiabilidad y minimicen los riesgos potenciales, fomentando la confianza y expresando nuestros valores compartidos.

Las entidades socias del BAIC somos conscientes de la importancia de los aspectos éticos en el desarrollo, uso e implementación de IA y de la necesidad de aplicar directrices que eviten cualquier tipo de riesgo potencial para las personas, las entidades, la sociedad en general o el medioambiente.

Aun cuando el RIA aún no es de plena aplicación, el ecosistema vasco de IA considera importante estar preparados y adoptar los principios éticos que reflejan los valores y las preocupaciones planteadas por dicha normativa, por la guía "Directrices éticas para una IA fiable" [<https://op.europa.eu/s/yUf5>] elaborada por el grupo de personas expertas de la Comisión Europea, por los principios de la OECD sobre IA actualizados en mayo del 2024 [<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>] y por las recomendaciones de la UNESCO [https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa]. Al anticiparnos a la aplicación plena de esta normativa, queremos demostrar un compromiso proactivo con los estándares éticos y legales que se establecerán en el futuro cercano.

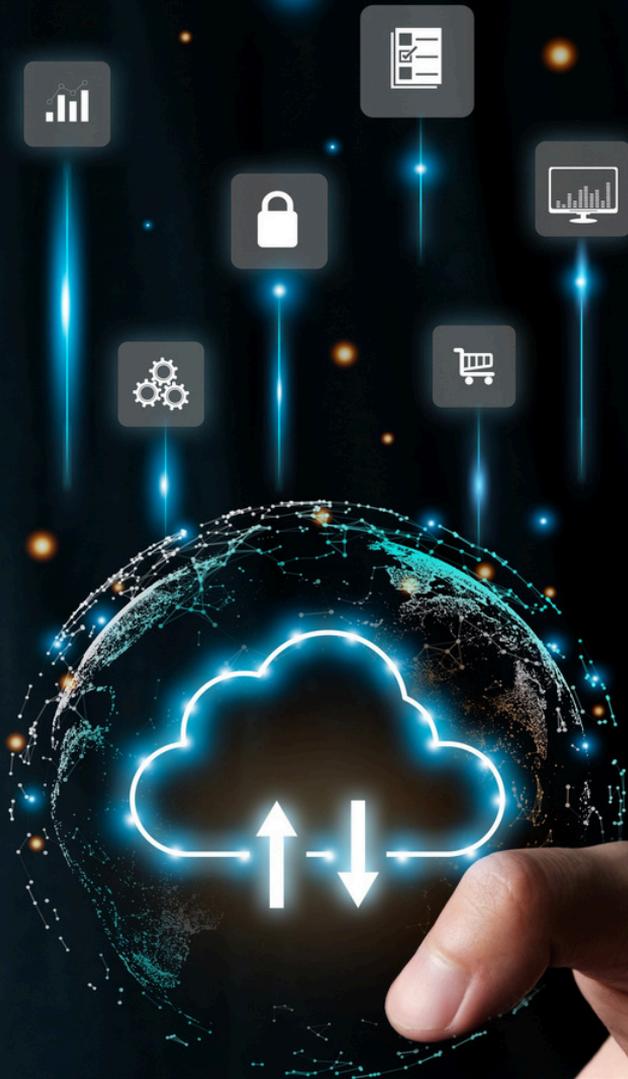
Este enfoque se basa en el apoyo voluntario y unilateral de este código ético por parte de las organizaciones del ecosistema de IA en Euskadi. Al ser un código apoyado

voluntariamente sin capacidad prescriptiva ni sancionadora, permite a las organizaciones adaptar sus políticas y prácticas internas a estos principios éticos, pero sin dejar de aspirar a cumplir con los requisitos que se establecerán en la futura normativa.

Es importante destacar que la anticipación y la adopción temprana de estos principios éticos no solo nos posiciona como líderes en el ámbito de la IA responsable en Euskadi, sino que también nos ayuda a establecer una base sólida para el desarrollo de tecnologías de IA responsables y confiables. Al demostrar nuestro compromiso con la ética, buscamos fomentar la confianza pública, minimizar los riesgos potenciales asociados a su uso e implementación y maximizar los beneficios para todos los actores interesados e involucrados en el ecosistema de IA en Euskadi.

Este documento representa la visión y compromiso del ecosistema con la Inteligencia Artificial responsable y establece los cimientos éticos sobre los cuales construiremos un futuro sostenible y confiable en el ámbito de la IA en Euskadi.

La elaboración de este documento inicia un proceso de responsabilidad en el desarrollo, uso e implementación de la IA que podrá concretarse en la adopción de normativas, códigos éticos internos por parte de los distintos agentes, desarrollo de actividades conjuntas de difusión, sensibilización y concienciación para el desarrollo, uso e implementación de una Inteligencia Artificial responsable, y otras acciones similares.



Consideraciones éticas fundamentales

2. Consideraciones éticas fundamentales

Existen multitud de documentos, análisis, reflexiones y guías que durante los últimos años han recogido distintas visiones e inquietudes en torno a la ética en la Inteligencia Artificial. Dado el carácter práctico y sencillo de este documento y tras un estudio pormenorizado de distintos marcos éticos, se resaltan cinco principios recurrentes y que el ecosistema vasco considera de especial relevancia:

Respeto de la autonomía humana

Los derechos fundamentales en los que se apoya la UE van dirigidos a garantizar el respeto de la libertad y la autonomía de los seres humanos. Las personas que interactúen con sistemas de IA deben poder mantener una autonomía plena y efectiva sobre sí mismas y ser capaces de participar en el proceso democrático. Los sistemas de IA no deberían subordinar, coaccionar, engañar, manipular, condicionar o dirigir a los seres humanos de manera injustificada. En lugar de ello, los sistemas de IA deberían diseñarse de forma que aumenten, complementen y potencien las aptitudes cognitivas, sociales y culturales de las personas. La distribución de funciones entre los seres humanos y los sistemas de IA debería seguir principios de diseño centrados en las personas, y dejar amplias oportunidades para la elección humana. Esto implica garantizar la supervisión y el control humano sobre los procesos de trabajo de los sistemas de IA. Para alcanzar dicho objetivo, debemos evitar el uso de agentes IA con la capacidad de tomar acciones y ejecutar cambios en el mundo físico y virtual sin aprobación humana.

Los sistemas de IA también pueden transformar de un modo fundamental el mundo del trabajo. Si bien existen amenazas como la vigilancia en el puesto de trabajo o la precariedad laboral, los sistemas de IA deberían ayudar a las personas en el entorno profesional complementando, mejorando y aumentando las capacidades creativas y de tipo cognitivo o incluso aumentando su seguridad. Además, la transformación de los empleos generará empleos generará nuevos puestos donde las capacidades humanas sean más útiles y donde las personas se sientan más valoradas y realizadas, sustituyendo tareas repetitivas de escaso valor por otras más satisfactorias para ser humano.

Prevención del daño

Los sistemas de IA no deberían provocar daños (o agravar los existentes) ni perjudicar de cualquier otro modo a los seres humanos. Esto conlleva la protección de la dignidad humana, así como de la integridad física y mental. Todos los sistemas de IA y entornos en los que operan deben ser seguros. También deberán ser robustos desde el punto de vista técnico, y debería garantizarse que no puedan destinarse a usos malintencionados. Las personas vulnerables deberían recibir mayor atención y participar en el desarrollo y despliegue de los sistemas de IA. Se deberá prestar también una atención particular a las situaciones en las que los sistemas de IA puedan provocar efectos adversos (o agravar los existentes) debido a asimetrías de poder o de información, por ejemplo, entre empresas y personas trabajadoras, entre empresas y personas consumidoras o entre gobiernos y ciudadanía. La prevención del daño implica asimismo tener en cuenta el entorno natural y a todos los seres vivos. Para alcanzar dicho objetivo, debemos asegurar de manera eficiente que la IA que utilizamos está alineada con los derechos humanos.

Justicia

El desarrollo, despliegue y utilización de sistemas de IA debe ser equitativo. Pese a que reconocemos que existen muchas interpretaciones diferentes de la equidad, creemos que esta tiene tanto una dimensión sustantiva como procedimental. La dimensión sustantiva implica un compromiso de garantizar una distribución justa e igualitaria de los beneficios y costes, y asegurar que las personas y grupos no sufran sesgos injustos, discriminación ni estigmatización. Si se pueden evitar los sesgos injustos, los sistemas de IA podrían incluso aumentar la equidad social favoreciendo incluso la integración de grupos minoritarios. También se debería fomentar la igualdad de oportunidades en términos de acceso a la educación, los bienes los servicios y la tecnología. Del mismo modo se debería fomentar la igualdad en el impacto de los beneficios que garanticen una sociedad más justa, inclusiva y equitativa equilibrando intereses privados con sociales. Además, el uso de sistemas de IA no debería conducir jamás al engaño de las personas afectadas ni a que se limite su libertad de elección. Para alcanzar dicho objetivo, debemos asegurar de manera eficiente que la IA que utilizamos está alineada con los derechos humanos. Asimismo, la equidad implica que los profesionales de la IA deberían respetar el principio de proporcionalidad entre medios y fines, y estudiar cuidadosamente cómo alcanzar un equilibrio entre los diferentes intereses y objetivos contrapuestos. La dimensión procedimental de la equidad conlleva la capacidad de oponerse a las decisiones adoptadas por los sistemas de IA y por las personas que los manejan, así como de tratar de obtener compensaciones adecuadas frente a ellas. Con este fin, se debe poder identificar a la entidad responsable de la decisión y explicar los procesos de adopción de decisiones.

Confiabilidad y Responsabilidad

La *confiabilidad y responsabilidad* son ingredientes fundamentales para garantizar que la IA opere de manera segura, ética y alineada con los derechos humanos. Para ello, debe asegurar algunos principios esenciales.

La IA debe ser *interpretable*, diseñándose de manera que sus procesos internos puedan ser comprendidos y analizados. Debe ser transparente, para que los procesos, modelos y datos utilizados sean accesibles y comprensibles. También debe ser *explicable*, capaz de proporcionar razones comprensibles para sus decisiones y predicciones. Sin olvidarse de ser *auditable*, es decir, trazable y evaluable mediante auditorías técnicas, regulatorias y éticas. Por otra parte, también se le debe exigir un *alineamiento* con los derechos humanos, los principios éticos y las normativas aplicables, garantizando que sus objetivos y decisiones reflejen principios de justicia, equidad y bienestar humano.

En el cumplimiento de estos objetivos de confiabilidad y responsabilidad, también nos encontramos con demandas asociadas, como que sea una IA *segura y robusta*, previniendo riesgos que afecten a la seguridad, la salud y los derechos fundamentales y garantizando su control técnico, y manejando adecuadamente la incertidumbre para lograr estas demandas. Por último, mencionar que podemos y debemos incrementar nosotros mismos el grado de confianza en la IA de la sociedad catalogando y declarando explícitamente aquel contenido que haya sido generado con IA.

Inclusividad, desarrollo sostenible y bienestar

Las partes interesadas deben participar de forma proactiva en la administración responsable de una IA fiable en busca de resultados beneficiosos para las personas y el planeta, como el aumento de las capacidades humanas y la mejora de la creatividad, el fomento de la inclusión de las poblaciones infrarrepresentadas, la reducción de las desigualdades económicas, sociales, de género y de otro tipo, fomentando así el crecimiento inclusivo y el bienestar.

Es importante recalcar la importancia de tener en cuenta el impacto medioambiental y los objetivos de desarrollo sostenible dentro del desarrollo y uso de los sistemas de Inteligencia Artificial. El entrenamiento, puesta en marcha y uso de estos sistemas debe ser respetuoso con el medio ambiente, minimizando el consumo de energía y favoreciendo el reciclaje de materias primas.



Aplicación de los principios éticos en el uso, desarrollo e implementación de la IA

3. Aplicación de los principios éticos en el uso, desarrollo e implementación de la IA.

3.1 Principios éticos

Las directrices éticas para una IA confiable elaborada por el grupo de personas expertas de alto nivel de la Comisión Europea establece siete requisitos clave para una IA confiable. Estos requisitos deben ser tenidos en cuenta desde el diseño de los sistemas de IA y son:

- 1. Acción y supervisión humanas:** Las personas deben tener la capacidad de supervisar y controlar el sistema de IA en todo momento. Los sistemas de IA deben estar diseñados de tal manera que permitan la intervención humana cuando sea necesario, posibilitando su autonomía y capacidad de decisión. Este requisito es indispensable en la confiabilidad de la IA, ya que se debe evitar la toma de decisiones de forma automática sin una intervención humana, sobre todo en aquellos sistemas considerados críticos. Asimismo debe tomarse conciencia de la tendencia a confiar automáticamente o en exceso en los resultados de salida del sistema (sesgo de automatización). La *acción humana* como el derecho a interactuar y tomar decisiones con conocimiento de causa, disponiendo de los conocimientos y herramientas necesarias para comprender los sistemas de IA e interactuar con ellos. Y la *supervisión humana*, como i) la habilidad de la persona supervisora para intervenir en cada decisión del sistema basado en IA y asumir la responsabilidad de las decisiones., ii) la capacidad de la persona para diseñar y monitorizar dicho sistema, y iii) la habilidad de la persona supervisora para supervisar la actividad global del sistema de IA (impacto económico, social, legal y ético), y garantizar que las decisiones tomadas por el sistema de IA puedan ser anuladas por el ser humano.
- 2. Solidez técnica y seguridad:** Los sistemas de IA deben mostrar una solidez técnica, que se traduzca en un desarrollo con enfoque preventivo con relación a los riesgos, comportándose de manera previsible, y reduciendo al mínimo el daño no intencionado y las consecuencias de daño intencionado. Deben mostrar una resistencia a los ataques y seguridad, protegiéndose de ataques contra el hardware o software, los datos, o los propios modelos de la IA. Deben contar con un plan de repliegue y seguridad general, estableciendo procesos dirigidos a evaluar y aclarar los riesgos asociados al uso del sistema de IA en cada uno de los ámbitos de aplicación. Deben contar con la precisión adecuada a la hora de, por ejemplo, formular recomendaciones o predicciones, indicando la probabilidad de error o el grado de incertidumbre en sus estimaciones. Y, por último, deben ser sistemas fiables y reproducibles.
- 3. Gestión de la privacidad y de los datos:** Los sistemas de IA deben garantizar la protección de la intimidad y de los datos, incluyendo la información proporcionada por las personas, así como la generada por su interacción con los sistemas. La calidad e integridad de los datos es un componente fundamental para garantizar el desempeño adecuado de un sistema basado en IA; la calidad posibilita el desarrollo de sistemas con rendimiento adecuado, mientras que asegurar la integridad evita la incorporación de datos malintencionados que interfieran en el comportamiento del sistema basado en IA. Por último, el acceso a los datos debe regirse por protocolos adecuados que garanticen el cumplimiento de la normativa.

4. **Transparencia:** Los sistemas de IA deben basarse en datos y procesos que sean *trazables*, también sus decisiones, facilitando así la auditabilidad y explicabilidad, ambos ingredientes esenciales. En concreto, la *explicabilidad* debe facilitar el entendimiento del proceso técnico de un sistema basado en IA, así como las decisiones humanas asociadas al mismo. Finalmente, la *comunicación* debe ser abierta, esto es, las personas tienen derecho a saber si están interactuando con un sistema basado en IA o no, y además informando de las limitaciones del propio sistema.
5. **Diversidad, no discriminación y equidad:** Los sistemas de IA deben evitar *sesgos injustos*, tanto desde el propio proceso de recopilación de los datos que se utilizarán para el entrenamiento del modelo, como desde el diseño algorítmico del sistema basado en IA. Además deben ofrecer *accesibilidad* y *acceso universal*, centrándose en la persona usuaria y diseñarse de manera que permitan que todas las personas puedan usarlos independientemente de su género, edad o capacidades y características. Por último, se debe incorporar en el ciclo de vida de desarrollo del sistema basado en IA a las personas usuarias y contando con la participación de todas las *partes interesadas*.
6. **Bienestar social y ambiental:** Los sistemas de IA deben ser diseñados de tal manera que sean *sostenibles* y *respetuosos* con el *medio ambiente*, evaluándose su diseño, desarrollo, despliegue y uso, así como la cadena de suministro que pueda estar involucrada. Además deben atender a su *impacto social*, haciendo un seguimiento del impacto en las relaciones humanas, y de su bienestar físico y mental. Finalmente, también debe considerar su impacto sobre la *sociedad en general* y la *democracia*.
7. **Rendición de cuentas:** Los sistemas de IA deben ser *auditables*, esto es, sus datos, algoritmos y procesos deben ser evaluables. Deben *minimizar los efectos negativos* y *ser capaces de notificarlos*, por ejemplo, a través de evaluaciones de impacto antes y después del desarrollo, despliegue y uso de los sistemas basados en IA. Deben *garantizar una búsqueda de equilibrios*, es decir, deberían identificar los intereses y valores subyacentes al sistema basado en IA. En caso de que surgiesen conflictos, deben explicitar cómo se ha llevado a cabo la búsqueda de dicho equilibrio entre ellos, y evaluarlo en términos del riesgo que plantea para los principios éticos, incluidos los derechos fundamentales. Y, para terminar, deben incorporar un *mecanismo de compensaciones* que permita reparar a los afectados en caso de efectos adversos no deseados.

3.2 Rol de desarrollador

Es necesario tener en cuenta las particularidades que afectan a las entidades desarrolladoras de sistemas basados en IA. En su caso, existen algunos énfasis éticos que es necesario tener en cuenta:

- **Aplicación de la ética desde el diseño:** Se deben incorporar los principios éticos desde el diseño y desarrollo de los sistemas de IA. Algunas de las consideraciones son el respeto por la privacidad, la consideración del bienestar social y medioambiental, mecanismos para evitar sesgos y la discriminación, respeto por la propiedad intelectual y la transparencia.
- **Validación de los sistemas:** Las entidades desarrolladoras deben asumir la responsabilidad de probar, testear y validar que sus sistemas se comporten según las especificaciones. Las consideraciones para tener en cuenta en este punto son la robustez del modelo, la precisión y la seguridad.
- **Explicabilidad:** Una documentación clara y accesible donde se explique cómo funciona el sistema y cómo toma decisiones es fundamental para garantizar sistemas transparentes y explicables. Además, existen un conjunto de métodos técnicos que permiten entender mejor las salidas de los agentes IA.
- **Cuantificación de incertidumbre:** Un sistema de IA robusto, debe funcionar correctamente con una alta variedad de entradas y situaciones. De modo que cuantificar y monitorizar la incertidumbre del sistema permite aumentar su robustez y minimizar los errores.
- **Resiliencia a ataques y ciberseguridad:** Los sistemas de IA, al igual que todos los sistemas de software, deben estar protegidos contra vulnerabilidades. Los ataques pueden dirigirse a los datos (envenenamiento de datos), al modelo (envenenamiento del modelo), a la información de entrada (ejemplos adversarios o evasión de modelos) o a la infraestructura subyacente, tanto el software como el hardware.
- **Mecanismos de auditabilidad:** La auditabilidad implica permitir la evaluación de algoritmos, datos y procesos de diseño. Esto no implica necesariamente que la información sobre los modelos de negocio y la propiedad intelectual relacionada con el sistema de IA deba estar siempre abiertamente disponible. La evaluación por parte de auditores internos y externos, y la disponibilidad de dichos informes de evaluación, pueden contribuir a la fiabilidad de la tecnología. En las aplicaciones que afecten a derechos fundamentales, incluidas las aplicaciones críticas para la seguridad, los sistemas de IA deben poder ser auditados de forma independiente.

3.3 Consideraciones normativas

La normativa europea de Inteligencia artificial establece un enfoque basado en riesgos para regular la IA. Según sea el potencial de riesgo de un sistema de IA, estos pueden ser clasificados en: Riesgo Inaceptable, Alto Riesgo, Riesgo Limitado y Riesgo Mínimo.

Esta regulación supone una norma de obligado cumplimiento que toda organización que haga uso de sistemas de IA incluidos dentro de su ámbito de aplicación deberá cumplir. Aun así, en un ejercicio de responsabilidad y proactividad, este documento ve necesario anticiparse a su plena aplicación.

Es fundamental garantizar que los principios éticos antes mencionados se apliquen de manera efectiva y por tanto a continuación se proporciona una breve descripción de cómo se pueden aplicar según el riesgo del sistema:

- **Riesgo Inaceptable:** En este nivel, los sistemas de IA pueden causar un daño significativo a los derechos fundamentales de las personas o a la sociedad. Por tanto, es crucial que se mantenga un fuerte énfasis en todos los principios éticos, pero sobre todo en la prevención del daño y la justicia. Estos sistemas deben ser prohibidos o su uso severamente restringido.
- **Alto Riesgo:** Los sistemas de IA que presentan un alto riesgo pueden tener un impacto significativo en la salud, la seguridad, los derechos fundamentales de las personas o en la sociedad. Deben ser diseñados con un alto grado de transparencia, explicabilidad y seguridad. El respeto a la autonomía humana es fundamental, garantizando que las decisiones importantes sean tomadas por humanos y no por máquinas.
- **Riesgo de Engaño:** Los sistemas de IA que presentan un riesgo de engaño pueden influir en los derechos y libertades de las personas. En este caso, la transparencia y la explicabilidad siguen siendo importantes, al igual que el respeto por la autonomía humana. No debe olvidarse que pueden existir sistemas de IA de alto riesgo que al mismo tiempo presenten riesgo de engaño (p.ej. sistemas de IA de alto riesgo dirigidos a interactuar con personas físicas).
- **Riesgo Mínimo:** Los sistemas de IA con riesgo mínimo tienen un impacto muy pequeño o nulo en los derechos individuales o sociales. Aunque los principios éticos siguen siendo importantes, el enfoque en su aplicación puede ser menos riguroso.

The background features a blue-toned digital environment with a central glowing brain icon containing the letters 'AI'. This brain is surrounded by a network of dashed white lines connecting various icons: a smartphone, a laptop, a padlock, a cloud with a circular arrow, and a group of three people. To the right, there is a vertical stack of blue folder icons connected by a dotted line. The overall aesthetic is futuristic and data-oriented.

Procesos para la implementación y actualización de este documento

4. Procesos para la implementación y actualización de este documento.

La importancia de este Código ético recae directamente en su apoyo e implementación dentro del ecosistema de IA de Euskadi. Siendo un documento de libre apoyo, no es labor de BAIC - Basque Artificial Intelligence Center, auditar o comprobar su cumplimiento, pero se invita a las entidades que apoyen el mismo a hacer autoevaluaciones internas que garanticen el cumplimiento del Código en todo el ciclo de vida de los sistemas de IA.

Su apoyo implica la puesta en marcha de procesos orientados a su adecuada implementación, seguimiento, comunicación (interna y externa) y revisión, para lo que se insta a promover entre las organizaciones miembros de BAIC y el ecosistema vasco de IA estrategias de colaboración y el intercambio de buenas prácticas con relación a la aplicación de estos principios éticos.

Además, debido a los rápidos avances en el desarrollo de sistemas de IA y su aplicación, es de vital importancia mantener el contenido de este Código debidamente actualizado. Para ello, se establece un comité de personas expertas dentro de BAIC que se encargue de su revisión y mantenimiento de forma anual. Dicho comité será formado por personas representantes de administraciones públicas, empresas desarrolladoras de IA, empresas usuarias de IA y centros científico-tecnológicos y de investigación afines a los campos de la ética o la tecnología.

Asimismo, se asume el compromiso por parte de BAIC de hacer fácilmente accesible este Código y comunicar de forma clara para el público en general y estableciendo un canal en la dirección baic@baic.eus a través del cual recibir comentarios (incluyendo cuestiones éticas que hayan podido surgir) y sugerencias de las partes interesadas.



Recomendaciones y siguientes pasos

5. Recomendaciones y siguientes pasos

5.1 Importancia de la ética en la IA

La Inteligencia Artificial ha llegado para quedarse y va a transformar la manera en la que trabajamos, educamos e incluso nos relacionamos. Sin embargo, este potencial transformador viene de la mano de desafíos y riesgos que tenemos la responsabilidad de mitigar aplicando nuestros valores éticos compartidos y respetando los derechos fundamentales de las personas.

Para asegurar que la IA sea utilizada de manera ética, responsable y segura, nace este Código de apoyo voluntario en el seno de BAIC.

Al apoyar este Código ético, las entidades socias de BAIC y el ecosistema vasco de IA pretenden que Euskadi sirva como ejemplo de cómo la IA puede ser desarrollada y utilizada de manera ética, justa y responsable. Al hacerlo, se persigue garantizar que la IA sea una fuerza transformadora que busque el bien y que beneficie a todas las personas y entidades miembro de nuestra sociedad.

5.2 Invitación al apoyo, implementación y difusión

Desde BAIC se invita a todas las organizaciones del ecosistema de IA en Euskadi a apoyar este Código y a iniciar acciones para su implementación y difusión. Al hacerlo, se establece una voluntad conjunta de desarrollar y utilizar la IA de una manera que respete los valores compartidos, fomente la confianza y promueva el beneficio para todos y todas.

5.3 Recomendaciones y siguientes pasos

A pesar de no ser labor de BAIC la acción o seguimiento de su cumplimiento, se establecen una serie de recomendaciones que las organizaciones pueden utilizar para implementar este Código dentro de su estructura.

- 1. Compromiso de la Dirección:** Es fundamental que la Dirección esté plenamente comprometida en el cumplimiento del Código ético de BAIC. Su apoyo y liderazgo es esencial para fomentar una IA responsable en toda la organización.
- 2. Creación de un Comité de Ética:** Establecer un comité o grupo de trabajo encargado de supervisar y orientar la implementación del Código. Este comité puede participar en el diseño de los proyectos desde el inicio o servir de consultoría ética.
- 3. Formación y concienciación:** Desarrollar programas de formación para educar y sensibilizar sobre la importancia del Código ético y de cómo aplicarlo a su trabajo diario.
- 4. Participación y colaboración externas:** Participar en redes y foros sobre ética en la IA para compartir experiencias, aprender de otras entidades y estar al día de la últimas tendencias y prácticas.
- 5. Transparencia:** Comunica abiertamente el apoyo de tu organización al Código ético. Esto puede incluir actos, publicaciones en redes sociales y otros medios de comunicación.

La implementación exitosa de un Código ético en IA requiere un esfuerzo coordinado y un compromiso a largo plazo con los principios éticos, adaptándose a los cambios continuos en el campo de la IA.