POLÍTICA GENERAL PARA EL USO DE IA GENERATIVA EN PROCESOS ADMINISTRATIVOS DE LA AEPD

VERSIÓN: 27 DE NOVIEMBRE DE 2025

Índice

1. INTRODUCCIÓN

El Plan Estratégico 2025-2030 de la Agencia Española de Protección de Datos (AEPD) apuesta por una política de *IA first*, promoviendo el uso seguro y responsable de la inteligencia artificial en todos los ámbitos en que resulte posible. La Agencia comparte la convicción de que la incorporación de la IA —y, en particular, de la inteligencia artificial generativa (en adelante IAG)— debe integrarse como un proceso normal en el funcionamiento de las administraciones públicas, al igual que en otros sectores de la sociedad. El objetivo es alcanzar la máxima eficiencia y calidad en el ejercicio de las funciones públicas, aprovechando las capacidades que ofrece para mejorar los procesos y servicios, en cumplimiento del principio constitucional de eficacia y de los mandatos constitucionales y legales de eficiencia y mejora continua que orientan la actuación administrativa.

La AEPD aspira a convertirse en un referente institucional en el uso de sistemas inteligentes aplicados a la administración pública, demostrando que la innovación tecnológica puede convivir con el cumplimiento normativo, la protección de los derechos fundamentales y la promoción de una cultura organizativa moderna, abierta al cambio y preparada para los retos del futuro digital.

El presente documento, en esta su primera versión, establece las bases para una política institucional de implementación y uso responsable de servicios de Inteligencia Artificial Generativa en los procesos administrativos de la AEPD –sean procesos que impliquen, o no, datos personales (tratamientos) –, orientando su despliegue progresivo y eficaz. Esta política se aprueba en ejercicio de las facultades de autoorganización y en el marco de la independencia de la AEPD, y forma parte de la Política de Información de la Agencia[1].

La política general descrita en este documento promueve, en el ámbito interno de la Agencia, la transparencia, la seguridad y la confianza en la implementación de la inteligencia artificial por la AEPD, con las garantías adecuadas en los tratamientos de datos personales, no personales o la combinación de ambos, y con un enfoque integral y conforme a derecho en el uso de la IA. Se trata de una política interna, aplicable exclusivamente a la AEPD, que no tiene carácter interpretativo respecto del Reglamento de Inteligencia Artificial[2] ni de otras normas europeas o nacionales. Esta política no acredita, no presupone ni desarrolla obligaciones derivadas del Reglamento de Inteligencia Artificial, y queda expresamente fuera de cualquier función de análisis, aplicación o interpretación de dicho Reglamento, incluido lo relativo a la identificación de sistemas prohibidos o de alto riesgo[3] y a las obligaciones vinculadas a ellos. El alcance de esta Política se circunscribe, por tanto, al uso de IAG en los procesos administrativos de la AEPD, sin que pueda considerarse en ningún caso una verificación, evaluación, certificación o forma indirecta de aplicación del Reglamento de Inteligencia Artificial.

[1] La asignación de responsabilidades no ha de confundirse con la figura del responsable tal como se define en el RGPD.

[2] El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial, en la medida que sea aplicable a los sistemas de IA desplegados y a los modelos de uso general utilizados.

[3] Las referencias a “alto riesgo” o similares que pudieran aparecer en esta Política responden al uso habitual de esa expresión en ámbitos de protección de datos, gestión de riesgos o análisis organizativo. No implican en ningún caso guardan relación con la categoría de sistemas de alto riesgo definida por el Reglamento de Inteligencia Artificial

2. OBJETIVOS DE LA IMPLEMENTACIÓN DE LA IAG EN LOS PROCESOS DE LA AEPD

Los objetivos de la AEPD con relación al despliegue de sistema de IAG en los procesos de la AEPD, son:

- **Aumentar la eficacia, eficiencia y calidad de los procesos de la AEPD a través de la innovación:** Aumento que no ha de ser puntual, sino que debe ser sostenido y paralelo al despliegue de nuevas tecnologías de IAG.

- **Proteger los derechos fundamentales**: Protección de los derechos y libertades tanto del personal de la Agencia como de la ciudadanía en general, en particular con relación a la protección de datos personales y, más allá del estricto cumplimiento normativo, con base en el principio de responsabilidad proactiva.

- **Proteger la información sensible o confidencial de la AEPD:** A estos efectos, se entenderá como información sensible o confidencial a cualquier dato que, si se divulga o accede sin autorización, puede suponer un riesgo o perjuicio para personas físicas y jurídicas, o para los objetivos de la organización.

- **Garantizar la salud y seguridad en el trabajo:** El despliegue de sistemas IAG puede realizarse implementando medidas que directamente benefician y protegen a la persona trabajadora, evitando riesgos de cosificación, incertidumbre ante nuevos escenarios u otros riesgos cognitivos.

- **Garantizar la continuidad de procesos**: Asegurando que la redefinición tecnológica de procesos mantiene su disponibilidad y resiliencia.

- **Controlar los costes operativos y financieros:** La IAG supone una inversión en la organización y las soluciones que se desplieguen tienen que contemplar que no solo es una cuestión de ahorro sino de eficiencia estratégica, de forma que los factores económicos para que sean escalables y mantenibles.

- **Fortalecer la confianza de la ciudadanía en la AEPD:** Garantizando la coherencia en la aplicación de criterios y respuesta a la ciudadanía, y acompañando el aumento de eficacia con una mayor transparencia, explicabilidad y trazabilidad en las acciones realizadas.

3. CASOS DE USO EN EL ÁMBITO ADMINISTRATIVO DE LA AEPD

En el marco de esta política, se identifican escenarios donde los sistemas IAG aportan valor y eficiencia a los procesos administrativos desarrollados por la AEPD. Cada escenario se denomina “caso de uso” y supone implementar en un proceso de la AEPD uno o más sistemas de IA.

Existirán procesos que no traten datos personales, y otros que sí traten datos personales (tratamientos de datos según el RGPD). De cualquier modo, cada caso de uso requiere analizar el impacto que tiene el o los sistemas de IAG en todo el proceso, lo que incluye la interacción con otros

sistemas que no están basados en IAG[4]IA, los recursos humanos y material, y los procedimientos organizativos de dichos procesos.

Los casos de uso identificados muestran las principales aplicaciones de la IAG en los procesos internos de la AEPD, comunes en las administraciones públicas. Abarcan desde tareas de apoyo a la comunicación institucional, la redacción de documentos, la automatización ofimática o la elaboración de materiales formativos, hasta la generación de informes, resúmenes o traducciones de documentos de acceso público. También se contemplan aplicaciones orientadas a la mejora de la gestión interna, como asistentes normativos, herramientas de apoyo a la tramitación de procedimientos o sistemas inteligentes de seguimiento del plan estratégico. Casos de uso[5] similares pueden presentar un riesgo o impacto significativamente menor cuando no incorporan información con datos personales, información sensible o confidencial.

La siguiente tabla de casos de uso identificados no tiene carácter exhaustivo ni vinculante, sino ejemplificativo, y se actualizará de acuerdo con la evolución tecnológica, la normativa aplicable y las necesidades organizativas de la Agencia.

Cabe reiterar que esta política no evalúa ni clasifica los casos de uso en términos del Reglamento de Inteligencia Artificial. No obstante, y en todo caso, se considera que ninguno de los casos de uso pueda encajar en la categoría de sistemas de alto riesgo –ni, obviamente, prohibidos– definida por dicho Reglamento. A mayor cautela, si en una fase posterior de desarrollo o despliegue se apreciara que un caso de uso pudiera estar comprendido en alguno de los supuestos regulados por el Reglamento de Inteligencia Artificial, correspondería aplicar íntegramente el régimen jurídico previsto en dicho instrumento.

[4] Como pueden ser sistemas de recogida de datos, procesado, transmisión, almacenamiento o incluso de ayuda a la decisión no basados en sistemas IAG.

[5] Es importante no confundir el riesgo que puede existir en proceso (o tratamiento cuando hay datos personales) con el riesgo de un sistema IA. En muchos casos de uso de distinto riesgo se piensa usar el mismo sistema. Tampoco hay que confundir el riesgo que el uso de un sistema IA puede suponer para una organización (como el riesgo reputacional) con la clasificación de riesgo que tiene un sistema de IA de acuerdo al Reglamento (UE) 2024/1689.

Casos de Uso	Descripción
Estructuración, gestión o resumen de documentos generales y abiertos (documentos públicos)	Aplicación de modelos inteligentes para resumir, extraer información clave y transformar documentos de carácter público o no confidencial en formatos estructurados que faciliten su análisis o reutilización. Pueden generarse versiones de clasificación o análisis automatizado con fines de estudio o divulgación, garantizando en todo caso la anonimización y la exclusión de datos personales.
Traducción de documentos públicos	Facilitar la traducción de documentos públicos en diferentes idiomas. Permite traducir documentos redactados en lenguas extranjeras (por ejemplo, resoluciones de autoridades europeas) al español, o viceversa, adaptando el estilo de la traducción según el público objetivo.
Generación de contenidos de comunicación institucional	Asistencia integral a la producción y revisión de materiales de comunicación institucional.
Generación de esquemas, mapas conceptuales e infografías para la comunicación	Creación de esquemas, mapas conceptuales e infografías explicativas elaboradas a partir de información pública o de fuentes abiertas, para apoyar la comprensión y difusión de contenidos.
Generación material y contenidos multimedia interactivo y de comunicación	Desarrollo de contenido multimedia interactivo destinado a la educación y divulgación ciudadana, así como composición automática de música o sonido ambiental para acompañar vídeos o actos públicos institucionales o promocionales.
Generación de audios o vídeos a partir de contenidos y documentación abierta	Generación de locuciones o vídeos sintéticos, obtenidas exclusivamente a partir de documentación pública o no confidencial y sin datos personales, aplicables a audioguías, servicios telefónicos o materiales accesibles.
Elaboración de contenidos divulgativos o formativos	Apoyo en la creación de materiales de sensibilización y formación interna o externa sobre protección de datos, accesibles y adaptados a distintos perfiles.

Identificación de tendencias o patrones a partir de fuentes abiertas	Identificación de tendencias o patrones mediante el análisis automatizado de información abierta para el apoyo a la toma de decisiones.
Elaboración de gráficas, tablas e informes a partir de información de acceso público o no confidencial	Elaboración automática de gráficos, tablas e informes financieros o presupuestarios basados en datos de acceso público o no confidenciales, garantizando la exclusión de información personal o sensible.
Asistencia en la aproximación y preparación general de argumentos, estudios jurídicos y técnicos	Utilización de sistemas de IA generativa para el análisis y contraste de fuentes jurídicas, doctrinales o técnicas de carácter público o no confidencial, con el fin de elaborar marcos argumentales, estudios comparados, notas técnicas o hipótesis interpretativas. Estas herramientas apoyan la preparación de estrategias o enfoques jurídicos sin sustituir la valoración profesional ni implicar toma de decisiones automatizadas. Asimismo, pueden emplearse para el análisis exploratorio y sistemático de fuentes jurídicas o abiertas, la comparación de marcos normativos o doctrinales, y la elaboración de estudios generales que no involucren información confidencial ni datos personales.
Asistencia en la redacción inicial de elementos generales y aislados cuyas ideas luego puedan incorporarse a resoluciones, informes o guías técnicas	Utilización de sistemas de IA generativa para el análisis y contraste de fuentes jurídicas, doctrinales o técnicas de carácter público o no confidencial, con el fin de elaborar marcos argumentales, estudios comparados, notas técnicas o hipótesis interpretativas. Estas herramientas apoyan la preparación de estrategias o enfoques jurídicos sin sustituir la valoración profesional ni implicar toma de decisiones automatizadas. Asimismo, pueden emplearse para el análisis exploratorio y sistemático de fuentes jurídicas o abiertas, la comparación de marcos normativos o doctrinales, y la elaboración de estudios generales que no involucren información confidencial ni datos personales.

Asistencia en tareas de desarrollo y configuración de sistemas	La IA se ha convertido en una herramienta clave para tareas técnicas como scripting, generación de consultas SQL, construcción de expresiones regulares y resolución de dudas sobre software específico. Facilita gran parte del trabajo, permitiendo a los usuarios enfocarse en la revisión y ajuste fino en lugar de empezar desde cero. Esto es especialmente útil en entornos donde se manejan múltiples tecnologías y configuraciones avanzadas de sistemas.
Asistente interno normativo o doctrinal	Desarrollo de asistentes virtuales internos que faciliten la consulta rápida de legislación, resoluciones, informes jurídicos, criterios interpretativos de la Agencia, etc., mejorando el acceso al conocimiento organizativo. Pueden servir de apoyo para la inspección, para las distintas fases de tramitación de solicitudes de aprobación de códigos de conducta y las de solicitudes de acuerdos de transferencias internacionales, o para la elaboración de resúmenes anonimizados para apoyo a divulgación de contenidos, entre otras.
Transcripción de audio y vídeo procedente de fuentes abiertas sin información confidencial	Transcripción de contenidos multimedia de fuentes abiertas o no confidenciales para su incorporación a diferentes flujos de trabajo o estudios. Podría contener datos personales.
Transcripción de audio y vídeo que contenga información interna, privada o confidencial, en su caso de reuniones y apoyo a la generación de actas	Transcripción de reuniones internas, en su caso para apoyo a la generación de actas. Así como de audios particulares de entrevistas concedidas o intervenciones realizadas por el personal de la Agencia en actos o eventos y elaboración de resumen del texto resultante.
Estructuración, gestión o resúmenes de documentos administrativos internos o con datos personales	Aplicación de modelos inteligentes para resumir, extraer información clave y convertir documentos administrativos internos en estructuras normalizadas que mejoren su tramitación o análisis automatizado. En estos casos, debe aplicarse una anonimización completa o parcial de los datos personales y limitar el tratamiento a entornos seguros y autorizados, por ejemplo, para elaborar versiones anonimizadas destinadas a consultas de transparencia o informes internos.

Redacción de borradores, cartas, correos o notas internas con tono institucional	Utilización de sistemas inteligentes para elaborar propuestas iniciales de respuesta a la ciudadanía u organismos, o escritos agilizando tiempos de tramitación y garantizando coherencia en los mensajes institucionales.
Generación de borradores de respuesta a consultas para canales de atención al ciudadano, canal DPD y joven.	La utilización de RAGs y sistemas bien afinados permitirán acceder a información actualizada en tiempo real sobre todo el material producido por la AEPD para producir borradores de respuestas a consultas específicas de los canales de atención al ciudadano, canal del DPD y canal joven.
Clasificación y resumen de denuncias, reclamaciones, consultas y otras entradas.	Aplicación de modelos de procesamiento de lenguaje natural (PLN) para facilitar el tratamiento inicial de la información que llega a la Agencia, permitiendo su categorización, indexación y análisis preliminar.
Apoyo en el análisis de EIPD (Evaluación de Impacto en Protección de Datos)	Utilización de modelos expertos para realizar un primer triaje o apoyo documental en los informes de evaluación de impacto, proporcionando plantillas, criterios comunes o guías de análisis.
Gestión inteligente del plan estratégico	La automatización de la gestión del plan estratégico facilita el seguimiento en tiempo real de los indicadores relativos al cumplimiento de los objetivos y resultados. Permite automatizar la metodología escogida, optimiza la ejecución de la estrategia y permite la toma de decisiones basada en datos en tiempo real. Análisis de datos y visualización de resultados para seguimiento de planes e indicadores.
Asistencia en la redacción de resoluciones, informes o guías técnicas.	Uso de herramientas de IA generativa como apoyo a la elaboración inicial de borradores de documentos normativos y doctrinales, facilitando la estructuración de contenidos y aumentando la eficiencia en la producción documental relativa a casos específicos.
Sistemas de alertas inteligentes (priorización de denuncias, reclamaciones, notificaciones y otras entradas)	Desarrollo de sistemas de IA o RPA que permitan detectar y priorizar denuncias, brechas de datos o comunicaciones sensibles, incluyendo alertas automáticas para casos de alto impacto, colectivos vulnerables o situaciones que requieran una atención prioritaria a criterio de la Agencia, permitiendo así una gestión ágil y focalizada.

Soporte a la tramitación de expedientes y notificaciones de brechas de datos	La tramitación de expedientes y/o notificaciones de brechas de datos personales son procesos manuales asistidos por varias herramientas corporativas. La IAG permite acelerar tareas, desde la clasificación inicial de las entradas por registro, su categorización y extracción de información estructurada, hasta la elaboración de resúmenes y borradores.

Los casos de uso planteados no agotan el potencial de la aplicación de estas tecnologías en la organización, que podrán ampliarse progresivamente y que se incorporarán a la presente política una vez se identifiquen.

Antes de su implantación, cada caso de uso se desarrollará y analizará en un Anexo a esta política general con los siguientes criterios:

- Descripción extendida.
- División/Subdirección responsable.
- Impacto general estimado sobre los objetivos de la AEPD.
- Tipo de sistema recomendado.
- Riesgos por requisitos o implicaciones.
- Observaciones/obligaciones específicas.

4. ANÁLISIS DE LOS RIESGOS PLANTEADOS POR LA IAG

La implantación de inteligencia artificial generativa en los procesos del ámbito administrativo, en particular por su novedad, requiere un análisis de los riesgos que deben ser identificados y gestionados adecuadamente para cada caso de uso (o grupos de casos de uso).

Los riesgos se han gestionado en función de cómo pueden comprometer los distintos objetivos de la AEPD con relación al despliegue de sistema de IAG en los procesos de la AEPD, entre los que está, de forma prioritaria, la protección de los derechos y libertades de la ciudadanía. Las amenazas específicas que implican la inclusión de sistemas IAG en procesos de la AEPD y que ponen en riesgo los objetivos se identifican a continuación[6] sin perjuicio de los riesgos particulares que deban analizarse en cada proceso o tratamiento concreto en el que se apliquen los distintos casos de uso.

[6] Se desarrollan en un documento anexo.

Objetivos de la AEPD	Grupos de Amenazas
Aumentar la eficacia de los procesos de la AEPD a través de la innovación	• Ineficacia de los sistemas de IA • Inseguridad de la infraestructura y falta de continuidad de procesos • Interacción humana incorrecta, irresponsable o perjudicial con la IA
Proteger los derechos fundamentales	• Ineficacia de los sistemas de IA • Sesgo y discriminación • Impactos para los derechos y libertades con relación a la protección de datos: LIINE4DU • Inseguridad de la infraestructura y falta de continuidad de procesos • Divulgación de información no personal • Interacción humana incorrecta, irresponsable o perjudicial con la IA
Proteger la información sensible o confidencial de la AEPD	• Inseguridad de la infraestructura y falta de continuidad de procesos • Divulgación de información no personal • Interacción humana incorrecta, irresponsable o perjudicial con la IA
Garantizar la salud y seguridad en el trabajo	• Impactos para los derechos y libertades con relación a la protección de datos. • Interacción humana incorrecta, irresponsable o perjudicial con la IA • Impacto en los derechos del personal empleado.
Garantizar la continuidad de procesos	• Inseguridad de la infraestructura y falta de continuidad de procesos • Desgobierno y pérdida de integridad institucional
Controlar los costes operativos y financieros	• Desgobierno y pérdida de integridad institucional
Fortalecer la confianza de la ciudadanía en la AEPD	• Ineficacia de los sistemas de IA • Sesgo y discriminación • Impactos para los derechos y libertades con relación a la protección de datos. • Inseguridad de la infraestructura y falta de continuidad de procesos • Falta de transparencia y explicabilidad de las actuaciones basadas en IAG • Falta de coherencia ante situaciones similares o desviaciones en la aplicación de criterios vigentes.

No todos los procesos de la entidad tienen el mismo nivel de criticidad respecto al cumplimiento de los objetivos de la AEPD, por lo que se los distintos casos de uso se clasificarán en función del nivel de riesgo que presenten.

El análisis en detalle de estas amenazas y el impacto que pudieran tener en función del tipo de sistema IAG que se implemente en los procesos se desarrollará en un documento Anexo a esta política general.

5. GOBERNANZA, POLÍTICAS Y GESTIÓN DE LA IAG

Este apartado recoge el conjunto de medidas estructurales que implementa la AEPD para conseguir los objetivos planteados con la implementación de sistemas de IAG. Está formada:

- Por un modelo de gobernanza interna con relación a la IAG.
- Por el conjunto de políticas que determinan las medidas marco que guiarán la implementación de los casos de uso y que se adaptarán a la criticidad de los procesos y el impacto que pueda suponer la materialización de una amenaza.
- Por el conjunto de procedimientos básicos para implementar dichas políticas, sin perjuicio de extenderlos en función de las necesidades detectadas.

A) Gobernanza interna

Se establece un modelo de gobernanza de la implementación en los procesos de la AEPD de sistemas IAG que manejan datos personales o no personales[7]. Tiene como propósito alcanzar todos los objetivos planteados por la AEPD (ver apartado II).

La estructura de la gobernanza de la IA incluye la participación de todos los niveles de la organización, para conciliar prioridades, agilizar la resolución de conflictos, e involucra a actores externos y fomentar colaboraciones interinstitucionales promoviendo buenas prácticas, herramientas comunes y lecciones aprendidas.

En la AEPD, se establecen los siguientes roles:

- **Responsable de la Organización**, la autoridad que decide usar o desarrollar uno o varios sistemas IAG dentro de los casos de uso de la AEPD. En el caso de la AEPD representada por el Presidente.
- **Responsables funcionales de los casos de uso**, encargados de definir objetivos, requisitos y supervisar la eficacia. En el caso de la AEPD los Subdirectores Generales, los Directores de División, el responsable del Gabinete de Prensa y Comunicación y el responsable del Servicio Jurídico.

[7] La AEPD no pretende establecer interpretaciones sobre tratamientos de datos que no son de su competencia, pero sí está obligada, como cualquier otra organización, a implementar una política de información que cumpla con toda la normativa y con sus objetivos de eficacia y eficiencia.

- **Responsables técnicos**, encargados de la implementación, mantenimiento y seguridad de los sistemas. En el caso de la AEPD, la Secretaría General.

- **Delegado de Protección de Datos**, que velará por el cumplimiento del RGPD y la aplicación de la responsabilidad proactiva.

- **Responsables de seguridad de la información**, encargados de garantizar la confidencialidad, integridad y disponibilidad de los sistemas. En el caso de la AEPD, el Subdirector General Adjunto de Promoción y Autorizaciones.

- **Responsable IA**, que coordinará el despliegue estratégico, la supervisión, la interlocución transversal entre unidades y el seguimiento de buenas prácticas. En el caso de la AEPD, la División de Innovación Tecnológica, representada por su Director.

B) POLÍTICAS

La presente política general, en la inclusión de sistemas de IAG en los casos de uso se seguirán las siguientes políticas para su diseño, implementación, explotación y mantenimiento:

POLÍTICA DE SELECCIÓN DEL TIPO DE SOLUCIÓN IAG

Los sistemas de IAG podrían formar parte de los procesos de la organización con distintos grados de integración:

- Inclusión o modificación de una fase del proceso mediante IAG, sin que exista una integración en los sistemas de información de la organización, como puede ser el caso de la etapa de corrección de textos cuando se utilice mediante un servicio accesible a través de un navegador.

- Funciones integradas en herramientas ofimáticas o en herramientas de *workflow* que supongan la interacción con sistemas de IAG y posibles conexiones con herramientas externas cuando el usuario tiene pleno control de la información con la que interactúa la IAG. Por ejemplo, cuando un usuario tiene abierto un documento concreto y utiliza la IAG sobre ese documento para traducción, resumen u otros.

- Integración plena en el entorno ofimático corporativo, donde el sistema IAG es un elemento inseparable que interviene en todo el flujo de trabajo administrativo incluyendo todo tipo de herramienta del entorno y medios de almacenamiento, lo que implica posible acceso del sistema IAG a toda la información procesada en el entorno ofimático de la organización y conectividad con utilidades externas a través de Internet.

- Integración en la infraestructura TIC de la organización, a nivel de sistema operativo y comunicaciones.

A su vez, los sistemas de IAG permiten tres enfoques básicos para su implementación:

Enfoques	Fortalezas	Debilidades
Sistemas IAG de terceros desplegados en infraestructura fuera del control de la organización, utilizados como SaaS bajo sus términos de uso (Sistema Externo): Están gestionados y mantenidos por proveedores externos y están accesibles a través de plataformas en línea. A su vez, pueden estar integrados en sistemas más amplios. Pueden ser utilizados para implementar una fase en el procedimiento (acceso a través de navegadores a servicios como ChatGPT, Perplexity, Mistral, ALIA, etc.), o integrados en el entorno ofimático como Microsoft 365 Copilot.	• Ineficacia de los sistemas de IA • Facilidad de uso • Gran potencia • Interfaz vía web o API • Menor mantenimiento • Mayor evolución tecnológica	• Revelación de información personal, de los usuarios finales y ciudadanos, sensible y confidencial a terceros. • Posibilidad de perfilado de usuarios • Falta de control sobre los flujos de datos. • Falta de control sobre las versiones. • A largo plazo, falta de control de los costes financieros. • Difícil automatización de las políticas de uso por el personal de cada sistema IAG. • Posibilidad de alucinaciones y correlaciones irrelevantes. • Sin control de repetibilidad • Sin control sobre sesgos. • Posible carencia de trazabilidad en los flujos de datos • Sin posibilidad de auditar • Exposición a ataques a través de Internet: potenciales vulnerabilidades en interfaces, APIs y otros. • Cambios unilaterales en ToS y discontinuidad de producto. • Explicabilidad muy limitada.
Sistemas IAG desarrollados por terceros y desplegados en infraestructura bajo control de la organización (Sistema interno):	• Ineficacia de los sistemas de IA • Auditable • Posibilidad de trazabilidad de flujos de datos. • Protección desde el diseño de los flujos información	• Requieren mayor inversión inicial. • Requieren mayor capacitación del personal • Requieren mayor mantenimiento.

El modelo se implementa en la infraestructura propia o en una nube privada. Generalmente, aunque no limitado, utilizando modelos de pesos abiertos como Llama, Qwen, Gemma o Mistral. También soluciones bajo licencia comercial que se puedan desplegar íntegramente en infraestructura propia de la organización, incluyendo los modelos.	personal, de los usuarios finales y ciudadanos, sensible y confidencial. • Control sobre el entorno de ejecución. • Integración con sistemas internos. • Permiten un mayor diseño de interfaces a medida. • Control de costes financieros. • Permite desarrollar pruebas de explicabilidad controladas	• Posibilidad de alucinaciones y correlaciones irrelevantes. • Evolución tecnológica dependiente de recursos. • Poco control sobre sesgos.
Sistemas IAG desarrollados internamente o por terceros bajo especificaciones a medida y desplegados en infraestructura bajo control de la organización e integrado con sistemas internos (Sistema Ad-hoc): Ofrecen el máximo nivel de personalización y control. Incluyen modelos de código abierto sobre los que se realiza un proceso de fine-tuning adaptado a necesidades específicas.	Además de las ventajas del anterior: • Máximo nivel de adecuación a los casos de uso concretos. • Mejor eliminación de alucinaciones. • Con conocimiento específico integrado. • Control sobre sesgos. • Mayor explicabilidad.	• Requieren mayor inversión inicial. • Requieren mayor mantenimiento. • Implican un proceso de postdesarrollo con recursos propios y/o contrataciones externas. • Evolución tecnológica dependiente de recursos.

Cada uno de estos de estos enfoques de implementación, en combinación con los diversos niveles de integración, implica diversas ventajas e inconvenientes, plantea distintos riesgos para el cumplimiento de los objetivos de la presente política general y permite implementar con distinta eficacia las políticas que se despliegan a continuación.

Como se establece en el procedimiento para incorporar casos de uso, se deberá seleccionar el enfoque y nivel de integración más adecuado para la incorporación de sistemas IAG en cada caso de uso en función de la evaluación del riesgo para el cumplimiento de los objetivos de esta política general.

POLÍTICA DE TRATAMIENTO DE INFORMACIÓN PERSONAL Y SENSIBLE O CONFIDENCIAL

Cada caso de uso tendrá un grado distinto de acceso a información personal y sensible o confidencial, existiendo casos en los que dicho acceso será nulo. Esta circunstancia deberá ser cuidadosamente evaluada durante el procedimiento para incorporar cada caso de uso. En dicha evaluación ha de

analizarse, en particular, si se han establecido medidas que evitan el tratamiento de información personal del propio usuario del sistema IAG.

- Los casos de uso que impliquen el proceso por parte de un sistema IAG8 de información personal, sensible o confidencial se implementarán, en aplicación del principio de precaución:
  - Preferentemente en sistemas IAG internos o *ad-hoc.*
  - En caso de que la aproximación anterior impida la consecución de otros objetivos de la presente política general, se podrán implementar en sistemas IAG externos que proporcionen evidencias de cumplimiento de la presente política general, más allá de meras manifestaciones o compromisos contractuales.

POLÍTICA DE DISEÑO DE LOS CASOS DE USO

- Los casos de uso que precisen tratar información personal identificable y datos sensibles o confidenciales con los sistemas IAG, se implementaran en sistemas IAG que permitan que la organización mantenga el control operativo y la supervisión directa sobre las medidas de confidencialidad y las garantías de limitación de la finalidad
- En el diseño y aplicación de los casos de uso de IAG se analizará y verificará:
  - Que las herramientas empleadas presenten interfaces sencillas y entornos de trabajo comprensibles, adaptados al nivel técnico del personal usuario, con instrucciones visibles sobre el modo correcto de solicitar, revisar y reutilizar los resultados generados.
  - Que exista información o documentación clara y suficiente sobre el funcionamiento general del modelo, incluyendo información sobre el tipo y procedencia aproximada de los datos empleados en su entrenamiento, las limitaciones conocidas y los posibles sesgos identificados.
  - Que los contenidos generados (textos, imágenes, resúmenes o informes) sean revisados y contrastados por personal competente, utilizando fuentes institucionales o verificadas, y que el procedimiento establezca mecanismos de validación colaborativa cuando los resultados puedan incidir en decisiones o documentos oficiales.
- En los sistemas de IAG desarrollados o gestionados directamente por la AEPD se deberán incorporar mecanismos de trazabilidad y registro básico de las interacciones, [9] que permitan identificar los usos realizados, los perfiles de usuario y la finalidad declarada, sin conservar

[8] Puede que el caso de uso se implemente, por ejemplo, en un proceso que sea un tratamiento de datos personales, pero la IAG no se emplee para tratar dichos datos.

[9] Las referencias a la trazabilidad y al registro en esta política se emplean exclusivamente en el sentido de control interno, gestión organizativa y verificación básica del uso responsable de los sistemas. No deben entenderse como una remisión a los requisitos de trazabilidad, registro o documentación previstos en el Reglamento de Inteligencia Artificial para los sistemas de alto riesgo, ni como una evaluación o aplicación de dicho marco normativo.

innecesariamente el contenido generado. Estos registros facilitarán la supervisión interna y el cumplimiento de las políticas de uso responsable.

- En el caso de soluciones externas o integradas en plataformas no controladas por la AEPD, se adoptarán medidas complementarias de control organizativo y técnico, tales como la limitación del acceso a entornos previamente autorizados, la prohibición expresa de introducir información personal, confidencial o no publicada, y la incorporación de avisos visibles o recordatorios sobre el uso permitido. Podrá establecerse asimismo un registro básico de accesos y finalidades con el fin de garantizar la trazabilidad y asegurar un uso seguro y conforme a las normas internas.

- Los eventuales cambios sustanciales en el ámbito de un caso de uso, su impacto, las personas físicas afectadas, el rendimiento del modelo, etc., deberán tratarse como un nuevo caso de uso.

POLÍTICA DE DISPONIBILIDAD Y RESILIENCIA

- Desarrollo de planes de continuidad y respaldo, que en caso de fallo o indisponibilidad del sistema IAG aseguren el funcionamiento del proceso en el que se ha implementado el caso de uso.

- Selección e implementación de sistemas IAG de forma que no generen dependencia de un solo proveedor.

- En aquellos casos de uso en los que el sistema IAG juegue un papel crítico para la continuidad de procesos que, a su vez, sean claves para la organización, deben implementarse medidas que garanticen dicha continuidad. Por ejemplo, asegurarse la posibilidad de tener acceso a más de un sistema IAG, que haya una posibilidad real y eficaz de migrar entre sistemas IAG y con interoperabilidad entre la información que sea necesaria para la ejecución de los procesos.

- Control de la puesta en explotación. de nuevas versiones de sistemas IAG:

  - En sistemas de IAG externos, que esté garantizado por contrato la información sobre nuevas versiones, en particular el control de optar por la nueva versión, y la información con evidencias de pruebas de comportamiento del sistemas o nuevos límites y contexto de uso.

- En caso de desarrollo de sistemas internos:

  - Aislamiento de entornos de entrenamiento y ejecución para prevenir propagación de fallos o vulnerabilidades.

  - Entrenamientos en entornos seguros, con control de versiones y validación previa antes del paso a producción.

  - Uso de técnicas de fine tuning reversibles (como LoRA o Adapters) que permitan actualización o retirada de componentes específicos sin afectar al sistema completo

- Supervisión de los sistemas de RAG mediante mecanismos de validación de fuentes, borrado controlado y protección frente a inyecciones maliciosas En aquellos casos de uso

POLÍTICA DE TRANSPARENCIA CON RELACIÓN AL USO DE IAG

Con relación a la transparencia:[10]

- Se documentarán los procedimientos, su ejecución y las decisiones realizadas en el marco de esta política general, garantizando su trazabilidad y conservación.

- Inclusión obligatoria de los sistemas IAG en el inventario de activos digitales del organismo, clasificando su criticidad, finalidad y relaciones con otros sistemas, accesible a todo el personal.

- En los procesos de selección o desarrollo de sistemas IAG se exigirá la incorporación de mecanismos de control de accesos, registro de uso y trazabilidad, especialmente en entornos que puedan conectarse con documentación interna o sensible (por ejemplo, sistemas RAG o plataformas documentales).

- Se establecerá un proceso documentado de gestión de incidentes con relación a la IAG.

- Los interfaces y entornos de trabajo deberán hacer visible al usuario cuando está interactuando con un sistema IAG, e incluir mensajes o recordatorios sobre las condiciones de uso y la necesidad de revisión humana de los resultados.

- La AEPD realizará un seguimiento continuo del uso de la IAG mediante indicadores de uso responsable y calidad de resultados, verificando -además- el cumplimiento de las condiciones contractuales, las garantías de seguridad y la confidencialidad acordadas con los proveedores. Este seguimiento se limitará al uso interno en la AEPD, sin incluir la auditoría de los modelos ni de los datos empleados en su entrenamiento.

POLÍTICA DE EXPLICABILIDAD

En aquellos sistemas IAG empleados directa o indirectamente para soporte a la decisión, para su selección en un caso de uso se tendrá en cuenta:

- La información que proporcione sobre las fuentes utilizadas.

[10] La referencia a la transparencia en esta política se emplea exclusivamente en sentido organizativo interno y no guarda relación con las obligaciones de transparencia previstas en el artículo 13 del Reglamento de Inteligencia Artificial para los sistemas de alto riesgo, ni debe entenderse como una interpretación o desarrollo de dicho régimen.

- La información que proporcione sobre cómo descarta determinadas fuentes o evita determinadas respuestas.
- La información sobre los pasos de razonamiento utilizada.
- La capacidad del usuario de seleccionar o restringir las fuentes.
- Si existe y se proporciona información sobre la calidad de la respuesta.
- Acceso al, o posibilidad de crear, un "Golden data set" o conjunto de datos de alta calidad para su uso como referencia para evaluar y validar el funcionamiento del sistema.
- Si se ofrece por el proveedor resultados de la evaluación realizada sobre las métricas de rendimiento que puedan ser oportunas para el caso de uso específico.

POLÍTICA CON RELACIÓN A LAS DECISIONES AUTOMATIZADAS Y SU SUPERVISIÓN

En el diseño de la implementación de un sistema IAG en un proceso se seguirán las siguientes políticas:

- En la implementación de sistemas IAG en los procesos de la AEPD, no existirán decisiones automatizadas basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
- En la implementación de sistemas IAG en los procesos de la AEPD se aplicará el principio de precaución de forma que no quede margen de duda en la aplicación del párrafo anterior.
- Todos los sistemas de soporte a la decisión empleados en procesos de la AEPD cuando afecte a derechos fundamentales, garantías procedimentales, tenga efectos jurídicos o puedan poner en riesgo los objetivos de esta política, se implementarán con las siguientes salvaguardas:
  - El proceso en el que se incluye el sistema de IAG ha de contemplar la validación y control humano previo, en cualquier caso[11].
  - Se realizará formación a los usuarios (ver política de recursos humanos y procedimiento de capacitación continua del personal) para cumplir de forma efectiva la supervisión humana.
  - En el procedimiento de supervisión se incluirá una evaluación de la carga de trabajo para determinar si es posible la intervención humana de forma efectiva.

[11] Las menciones a la supervisión humana en esta política se utilizan en el sentido propio de la gestión de riesgos, del control organizativo y, en su caso, de lo previsto en el RGPD para decisiones automatizadas. No deben interpretarse como una referencia a los requisitos de supervisión humana establecidos en el Reglamento de Inteligencia Artificial para los sistemas de alto riesgo ni como un análisis conforme a dicho Reglamento.

- Se aplicarán las recomendaciones de la Nota Técnica sobre supervisión humana del Supervisor Europeo de Protección de Datos[12].

POLÍTICAS CON RELACIÓN A LA PROTECCIÓN DE DERECHOS FUNDAMENTALES Y TRATAMIENTO DE DATOS PERSONALES

La evaluación y gestión de riesgos para los derechos fundamentales se regirá por la normativa aplicable en cada caso, incluidos, cuando proceda, los instrumentos previstos en el RGPD y en la legislación nacional sobre el sector público. Si, en una fase posterior, un sistema quedara comprendido en el ámbito del artículo 6, apartado 2, del Reglamento 2024/1689, de inteligencia artificial correspondería realizar la evaluación de impacto que dicho Reglamento exige, debiendo acudirse en ese supuesto a las guías, procedimientos o instrumentos específicos previstos en dicho marco normativo.

Asimismo, cabrá realizar una Evaluación de Impacto para la Protección de Datos cuando:

- el caso de uso suponga un tratamiento de datos personales que entrañe un alto riesgo para los derechos y libertades de las personas físicas (en este caso ya existirá una EIPD que se tendrá que revisar al cambiar parte de la naturaleza del tratamiento).

- el caso de uso suponga un tratamiento de datos personales al que se incorpore uno o varios sistemas de alto riesgo según el Reglamento 2024/1689 (RIA).

Más allá de cumplimiento de la normativa de protección de datos, en el diseño e implementación de un sistema IAG dentro de un proceso se tomarán las siguientes medidas:

- En cuanto a explotación de los sistemas de IAG en cada caso de uso:

  - Se configurará la capacidad de acceso a datos de la organización, y a datos relativos a los usuarios, por parte de los sistemas IAG aplicando el principio de minimización y de conservación limitada de datos, tanto de metadatos como de la memoria de usuario, de acuerdo con las necesidades del caso de uso.

  - Se diseñarán procedimientos o se implementarán herramientas que impidan la inclusión accidental de datos personales o confidenciales en los *prompts* o en los ficheros a los que el sistema IAG pueda acceder.

  - En sistemas IAG tipo RAG que requieran acceso desde servidores externos a datos de la organización hay que implementar técnicas de anonimización o seudonimización en las fuentes utilizadas reducir la exposición de información identificable.

- En cuanto al diseño de sistemas de IAG ad-hoc[13]:

[12] EDPS TechDispatch #2/2025 - Human Oversight of Automated Decision-Making
[13] Modelos de código abierto refinados mediante procesos de fine-tuning

- Aplicación de medidas que eviten el enriquecimiento no controlado de los conjuntos de datos (entrenamiento y recuperación), respetando los principios de limitación de finalidad y minimización.
- Aplicación de técnicas de anonimización y seudonimización antes del entrenamiento y en las fuentes utilizadas por sistemas RAG que impliquen la comunicación a sistema IAG externos.
- Consideración del uso de técnicas de Privacidad Diferencial en los datos empleados para evolución o ajuste fino, para reducir la posibilidad de memorización de datos personales en el modelo.
- Verificación documentada de que el modelo no incorpora datos personales o, en su caso, de que el acceso se limita estrictamente al principio de necesidad (need-to-know).

- Establecimiento de mecanismos técnicos y organizativos para proteger derechos y libertades de los interesados, tanto en el tratamiento como en la exposición de datos estructurados, anonimizados o documentos internos.

POLÍTICA DE CIBERSEGURIDAD

En la implementación de sistema IAG en los procesos se deberá asegurar:

- Los sistemas de IAG se someterán a categorización ENS y cumplirán los principios y medidas correspondientes al nivel resultante. Cuando el caso de uso implique información sensible, datos personales de categorías elevadas o funciones críticas, se adoptarán controles de 'nivel alto'.
- Además, se seguirán buenas prácticas de ciberseguridad reconocidas, tanto en el sector público como en el ámbito tecnológico general[14], que sean específicas con relación al uso de sistemas IAG y de acuerdo con el riesgo para la obtención de los objetivos de esta política general. En particular, en cumplimiento del artículo 32 del RGPD.
- El Responsable de IA monitorizará las nuevas amenazas y vulnerabilidades del estado del arte y el contexto de las soluciones IAG y el Responsable Técnico en los sistemas IAG concretos implementados en la organización. La implementación de sistemas IAG en los casos de uso se tendrá que revisar ante la severidad de las nuevas amenazas y vulnerabilidades detectadas.
- Aplicación de la Política de Información y seguridad de la AEPD.
- El uso de los sistemas de IAG se ajustará a las políticas corporativas de control de accesos y registro de actividad de la AEPD. En cada caso de uso se evaluará y documentará el esquema de identidades digitales que corresponda, determinando con qué perfil se accede —por

[14] Si la solución de IA que se implementa es la de Microsoft-Azure, además, se seguirá la Guía de Seguridad de las TIC CCN-STIC 884D.

ejemplo, identificación personal del empleado, cuentas genéricas de una unidad, identidades técnicas o de servicio, accesos temporales vinculados a proyectos u otras modalidades autorizadas que resulten adecuadas para el caso de uso o para las necesidades operativas de la organización—. La opción seleccionada deberá ser coherente con las funciones asignadas y con las necesidades específicas del caso de uso.

- Inclusión de las particularidades de los sistemas IAG en el proceso de gestión de incidentes con relación a, por ejemplo, identificación de sesgos, problemas de rendimiento o de disponibilidad.

- Aislamiento de entornos críticos. Los sistemas que operen con información clasificada o de alto impacto para el cumplimiento de los objetivos de esta política general deberán estar aislados de forma lógica o física del resto de redes, especialmente de internet.

POLÍTICA DE CONTRATACIÓN

En la contratación de soluciones IAG, especialmente cuando se trate de servicios externos o en la nube, se evaluarán de forma previa y documentada, al menos, los siguientes aspectos:

- El tratamiento de metadatos / cookies: qué datos técnicos y de uso se recolectan (logs, identificadores, telemetría, firma de dispositivo, etc.).

- Declaraciones explícitas de si el proveedor declara, no declara, o a qué nivel usa el contenido de las conversaciones/archivos para mejorar servicios/modelos y en qué condiciones.

- Existencia y alcance de mecanismos para excluir el contenido del usuario del entrenamiento (controles de cuenta).

- Posibilidad de configuración por el administrador de la cancelación de peticiones de opiniones o de grado de satisfacción a los usuarios finales (feedback).

- Posibilidad de configuración y control por el administrador de revisiones manuales realizadas por el proveedor de conversaciones o archivos y bajo qué garantías.

- La ubicación de datos: dónde pueden almacenarse/procesarse (EE. UU./UE/otras regiones)

- El cumplimiento RGPD.

- El tiempo de retención de datos: plazos o criterios para conservar chats y contenido del usuario.

- El control e información que se proporciona sobre el despliegue de nuevas versiones y sus características.

- La estabilidad del contrato y los términos de servicio. Evaluación de la estabilidad y previsibilidad de los términos del servicio, incluyendo cláusulas de continuidad, confidencialidad y seguridad.

- Si en una fase posterior se apreciara que la solución a contratar pudiera quedar dentro del ámbito de aplicación del RIA, corresponderá aplicar el régimen jurídico que dicho Reglamento establezca.

POLÍTICA DE RECURSOS HUMANOS CON RELACIÓN A LA IAG

- Será requisito imprescindible que cualquier persona usuaria de estas tecnologías reciba formación básica específica, y continua, sobre su correcto uso, sus limitaciones, buenas prácticas y riesgos asociados teniendo en cuenta, entre otros, el contexto de los casos de uso y de las personas o los colectivos de personas previsiblemente afectadas.

- Se incluirá en el plan anual de formación de la AEPD, y previa consulta al Responsable de IA, la ejecución de tres tipos de capacitación continua del personal con los siguientes aspectos:

  - Sobre la presente política general.

  - Sobre cada uno de los sistemas AIG que sean necesarios para realizar sus funciones. En particular, sobre *prompt engineering*, interpretación de salidas, identificación de sesgos y errores, y gestión de incidentes, entre otros.

  - Capacitación técnica formación tecnológica para equipos TIC en diseño, mantenimiento y control de sistemas automatizados e inteligentes sobre los sistemas de inteligencia artificial y que permita identificar oportunidades y riesgos.

- Se dispondrán de forma online guías de uso y material de formación para el personal, incluyendo la presente política general.

- Se establece un canal para comunicación bidireccional con el personal por parte de Recursos Humanos, más allá de la gestión de incidentes, para informar de cambios en la funcionalidad o nuevos riesgos, evitar incertidumbre o malentendidos entre el personal, además de para recoger sus sugerencias sobre nuevas oportunidades y posibles casos de uso.

- En el plan de supervisión incluirá el análisis de si la introducción IAG se acompaña de una sobrecarga de trabajo, sustitución de tareas sin planificación o pérdida de funciones sin reubicación.

POLÍTICA DE USO PARA EL PERSONAL

- La utilización de sistemas IAG para la ejecución del trabajo sigue las mismas restricciones que se aplican para cualquier sistema o dispositivo personal con relación a la Política de Seguridad de la AEPD.

- La utilización de sistema IAG estará restringida a las personas que hayan recibido la formación adecuada, en particular, sobre estas políticas.

- No utilizar un sistema IAG que no se haya registrado en el inventario de sistemas IAG.

- Los sistemas IAG deben ser usados únicamente para los propósitos establecidos en cada caso de uso, y dentro de los límites de las capacidades indicados en la documentación.
- En la distribución interna de material generado con IAG, se comunicará el uso de IAG y en qué grado el contenido está completamente generado por IAG.
- Todo contenido generado por IAG será revisado por la persona usuaria. Si está dirigido a superior jerárquico o destinado a publicarse tendrá que pasar una revisión interna por pares.
- Los resultados generados por sistemas IAG deberán ser contrastados con fuentes fiables, documentación interna o validación colaborativa, especialmente cuando afecten a procesos críticos o decisiones relevantes para la ciudadanía o entidades.
- Se minimizará a los estrictamente necesarios el uso en sistemas IAG externos el uso de información sensible no personal, como referencias institucionales, nombres vinculados a incidentes graves o documentos internos, aunque no contengan datos personales, que puedan dañar la imagen corporativa o la estrategia institucional propia o de terceros.
- En el uso de los sistemas IAG se aplicarán las políticas corporativas de control de accesos y registro de actividad de la AEPD, ajustando su configuración al caso de uso correspondiente y lo señalado en el apartado de Política de seguridad.
- Casos de uso de especial sensibilidad o complejidad pueden precisar de políticas o términos de uso específicos que extiendan lo establecido en este documento, que deberán ser respetadas por los usuarios.

POLÍTICA DE SUPERVISIÓN DE ESTA POLÍTICA

- Se establece un procedimiento de supervisión de cumplimiento de esta política general.
- Se establece una supervisión periódica de todos los casos de uso.
- Se establece un procedimiento de gestión de incidentes de IAG integrado en el sistema de gestión de incidentes de la AEPD.

C) PROCEDIMIENTOS

PROCEDIMIENTO DE REDACCIÓN APROBACIÓN Y REVISIÓN DE ESTA POLÍTICA GENERAL

- Esta política general será elaborada y mantenida por el Responsable IA siguiendo las directrices del Responsable de la Organización.
- Se someterán a revisión previa del DPD, los Responsables funcionales, técnicos y de seguridad de la información.
- Se someterán a la aprobación del Responsable de la Organización.

- El Responsable IA iniciará un ciclo de revisión de las políticas cuando:
  - Lo establezca el Responsable de la Organización.
  - Se produzcan incidentes que comprometan el cumplimiento de los objetivos de estas políticas.
  - Se identifiquen nuevos casos de uso.

PROCEDIMIENTO PARA INCORPORAR UN CASO DE USO

Los procedimientos descritos a continuación se aplicarán con un enfoque proporcional y flexible, en función de la naturaleza y complejidad del caso de uso. Podrán utilizarse plantillas o mecanismos simplificados, y elaborarse documentación común para varios casos de uso de características similares, siempre que se garantice la trazabilidad de las decisiones, la identificación de los responsables y la coherencia con esta política general.

- Identificación de necesidades por el Responsable Funcional en el marco de los procesos de la AEPD.
- Primera evaluación y, en su caso, diseño por el Responsable de IA, que incluirá:
  - Un análisis de riesgo con relación a las amenazas identificadas en esta política y las propias del proceso en el que se incluya el caso de uso.
  - Realización de las oportunas Pruebas de Concepto.
  - Una recomendación sobre si incluir IAG, y en su caso, el tipo de entorno a elegir.
  - Un diseño del proceso del caso de uso que contemple la implementación de las políticas anteriormente señalada.
- Revisión de la evaluación por el DPD (si procede), Responsable Técnico, de seguridad y Gabinete Jurídico (si procede) para determinar el cumplimiento normativo (tanto de protección de datos como de cualquier otra normativa aplicable).
- El Responsable Funcional elaborará un documento con los requisitos de diseño del caso de uso que elevará al Responsable de la Organización, que incluya entre otros:
  - Documentación de cumplimiento normativo (tanto de protección de datos como de cualquier otra normativa aplicable).
  - Aplicación de la política general.
  - Identificación de las necesidades de transparencia, explicabilidad, medidas con relación a decisiones automatizadas, formación y supervisión.
  - Criterios de validación y control de versiones.

- Aprobación por el Responsable de la Organización.

PROCEDIMIENTO DE DISEÑO Y DESPLIEGUE DE UN CASO DE USO

- El Responsable Técnico elaborará, a partir de los requisitos de diseño:
  - Elaboración de un plan de diseño del caso de uso.
  - Elaboración de un plan de despliegue, mantenimiento y retirada/sustitución.
  - Elaboración de un plan de verificación y validación.
  - Elaboración de un plan de contingencia.
  - Elaboración de guías, materiales, políticas y plan de formación específico (si aplicable).
- El Responsable Técnico lo elevará a la aprobación del Responsable de la Organización, que realizará las consultas que considere adecuadas para comprobar el cumplimiento de dicha política general.
- Una vez aprobado, el Responsable Técnico realizará la implantación y despliegue del sistema.
- El Responsable Técnico realizará y documentará el plan de verificación y validación, cuyos resultados contrastará con el Responsable de IA y, si resulta satisfactorio, elevará al Responsable de la Organización la decisión de poner el sistema en explotación.
- El Responsable Técnico registrará el sistema IAG en el inventario.

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

- Todo incidente se comunicará con *ticket* de soporte al Responsable Técnico.
- En la comunicación del incidente se ha de señalar:
  - Ineficacia de los sistemas de IA
  - Inseguridad de la infraestructura y falta de continuidad de procesos
  - Interacción humana incorrecta, irresponsable o perjudicial con la IA
  - Sesgo y discriminación
  - Impactos para los derechos y libertades con relación a la protección de datos.
  - Divulgación de información no personal
  - Desgobierno y pérdida de integridad institucional

- Falta de transparencia y explicabilidad de las actuaciones basadas en IAG
- Impacto en los derechos del personal
- Falta de coherencia ante situaciones similares o desviaciones en la aplicación de criterios vigentes.

- El Responsable Técnico comunicará el incidente al Responsable de IA que lo clasificará en leve o grave.
  - En caso de incidentes leves, el Responsable de IA emitirá las recomendaciones oportunas a los Responsable que considere oportuno.
  - En caso de incidentes graves, el Responsable de IA:
    - Lo comunicará de forma inmediata al Responsable de la Organización y, en su caso, al DPD.
    - Propondrá al Responsable de la Organización las acciones que sean necesarias.
    - El Responsable de la Organización, en caso de que el incidente afecte a un sistema de alto riesgo según el RIA, ejecutará las obligaciones que impone el art.73 del RIA.
    - Iniciará un proceso de supervisión.

PROCEDIMIENTOS DE SUPERVISIÓN DE ESTA POLÍTICA

- El proceso de supervisión se iniciará por decisión del Responsable de la Organización, y por indicación o consulta a los demás responsables.
- El proceso de supervisión se sugerirá por el Responsable de IA:
  - Anualmente
  - Existencia de un incidente grave.
  - Monitorización de las nuevas amenazas y vulnerabilidades del estado del arte y el contexto de las soluciones IAG[15].
  - Alerta de las herramientas automáticas de monitorización.

[15] Ataques conocidos en otras organizaciones, vulnerabilidad publicitada, cambios normativos de servicios dependientes de otros países, cambios contractuales, cambios en contextos políticos, económicos, o sociales relevantes.

- El procedimiento de supervisión seguirá un enfoque de riesgos, priorizando los casos de uso de mayor impacto o en los que haya sucedido un incidente grave.
- El procedimiento de supervisión se ejecutará mediante una auditoría interna o externa en función de la urgencia y disponibilidad de medios.
- Las acciones de supervisión comprobaran la aplicación de la presente política general, en particular:
  - Identificación de los incidentes y posible solución.
  - Revisión de cumplimiento normativo
  - Cumplimiento de los principios establecidos en las políticas, en particular con relación a la supervisión humana y usos permitidos.
  - Problemas identificados en la consecución de los objetivos de la AEPD a través de las métricas establecidas y posible solución.
  - Evaluación del Retorno de la Inversión (ROI) [16], en particular sobrecostes inesperados, impacto financiero interno por mantenimiento, licencias o escalabilidad mal dimensionada.
  - Evaluación periódica de vulnerabilidades. En función de la criticidad del sistema, se realizarán comprobaciones de la robustez del sistema IAG ante amenazas según el estado del arte (por ejemplo, ataques de *prompting*).
- El resultado del proceso de supervisión se documentará, incluyendo, si procede, recomendaciones sobre la adaptación del sistema IAG o de los procedimientos del proceso en el que se implementa el caso de uso, su sustitución o eliminación del sistema IAG.
- Se elevará a la decisión del Responsable de la Organización.

6. CONCLUSIONES

El presente documento establece una política general para la implementación, gobernanza y uso responsable de sistemas de inteligencia artificial generativa en el ámbito interno de la AEPD. Su finalidad es reforzar la capacidad tecnológica y organizativa de la Agencia, asegurando una transformación digital segura, ética y plenamente conforme con el marco normativo vigente. Como se ha señalado, esta política no es ningún instrumento de cumplimiento ni de desarrollo del Reglamento de Inteligencia Artificial. Asimismo y como se ha expuesto, no incorpora en ningún caso la clasificación de sistemas conforme a dicho Reglamento, incluidos los supuestos de alto riesgo. En conjunto, esta política busca situar a la AEPD como una institución pionera en el uso responsable,

[16] Entendida en términos de mejora del servicio a la ciudadanía antes que en términos monetarios.

legal y transparente de la inteligencia artificial y la automatización en la Administración Pública. La implantación progresiva de los sistemas, bajo una gobernanza sólida y con supervisión humana, permitirá a la Agencia mejorar su eficiencia y capacidad técnica sin renunciar a sus principios fundacionales: la defensa de los derechos, la protección de la privacidad y la ejemplaridad institucional.

Este documento proporciona, por tanto, una hoja de ruta realista, equilibrada y rigurosa para abordar la transformación tecnológica de forma segura, controlada y alineada con el interés público. Su implementación debe ir acompañada de un proceso continuo de evaluación, adaptación y mejora, que permita responder a los avances tecnológicos, los cambios normativos y las expectativas sociales, consolidando así una inteligencia institucional madura, ética y sostenible.

7. REFERENCIAS

- Agencia Española de Protección de Datos (2020) Adecuación al RGPD de tratamientos que incorporan IA
- Agencia Española de Protección de Datos (2020) Blog: Gobernanza y política de protección de datos
- Agencia Española de Protección de Datos (2021) Gestión del riesgo y evaluación de impacto en tratamientos de datos personales
- Agencia Española de Protección de Datos (2021) Requisitos para Auditorias que incluyan IA
- Agencia Española de Protección de Datos (2023) Aproximación a los espacios de datos desde la perspectiva del RGPD
- Agencia Española de Protección de Datos y Supervisor Europeo de Protección de Datos (2022) 10 malentendidos sobre el aprendizaje automático
- Asociación Española para el estudio, promoción y desarrollo del Marco de Competencias Profesionales en Contratación Pública (2024) Guía práctica para el uso de IA generativa por empleados públicos
- Comisión Europea (2019) Ethics guidelines for trustworthy AI
- Comisión Europea (2024) A strategic vision to foster the development and use of lawful, safe and trustworthy Artificial Intelligence systems in the European Commission
- Comisión Europea (2024) Guidelines for staff on the use of online available generative artificial intelligence tools
- Comité Europeo de Protección de Datos (2024) Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models

- Commission Nationale de l'Informatique et des Libertés (2025) AI and GDPR: the CNIL publishes new recommendations to support responsible innovation
- Commission Nationale de l'Informatique et des Libertés (2025) IA: Garantir la sécurité du développement d'un système d'IA
- European Medicines Agency (2024) Harnessing AI in medicines regulation: use of large language models (LLMs)
- Information Commissioner Office of UK () AI and data protection risk toolkit
- Information Commissioner Office of UK (2025) Internal AI Use Policy
- Office of the Privacy Commissioner for Personal Data of Hong-Kong (2025) Guidelines for the use of generative AI by employees
- Organización para la Cooperación y el Desarrollo Económico () Recomendación sobre la inteligencia artificial
- Organización para la Cooperación y el Desarrollo Económico y Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2024) G7 toolkit for artificial intelligence in the public sector
- Prof. Dr. Johan Wolswinkel - Council of Europe (2022) Artificial intelligence and administrative law
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD)
- Supervisor Europeo de Protección de Datos (2023) TechSonar - Large language models (LLM)