RESUMEN BÁSICO DE OBLIGACIONES Y RECOMENDACIONES PARA LA GESTIÓN DE IAG EN LA AEPD

En el marco de la 'Política General para el Uso de IA Generativa en Procesos Administrativos de la AEPD' publicada en noviembre de 2025 y del anexo que establece un marco práctico para la aplicación segura, ética y controlada de la IA en la AEPD, en diciembre de 2025, se listan de manera no exhaustiva las principales obligaciones y recomendaciones dirigidas a los órganos de decisión y los equipos a cargo de implantar casos de uso de IA Generativa (IAG) en los procesos y tratamientos de la organización:

Gobernanza

- Identificar de forma precisa los roles de decisión y ejecución conforme a la política interna de uso de IAG, especialmente los responsables funcionales y los responsables técnicos para la gestión y supervisión del funcionamiento del sistema IAG para cada caso de uso.
- Asegurar la aprobación previa de cada caso de uso antes de su implantación siguiendo el procedimiento de diseño y despliegue de nuevos casos de uso.
- Mantener un registro actualizado de los sistemas de IAG en uso en el inventario de activos digitales, documentando cómo operan, finalidad y nivel de riesgo.
- Definir y aplicar un procedimiento de gestión del ciclo de vida de los sistemas IAG desde la propuesta hasta su retirada, que aplique las medidas para garantizar el cumplimiento normativo proporcionales a los riesgos de los procesos y tratamientos en los que se incluye.

Diseño y desarrollo de casos de uso

- Considerar el uso de IAG como apoyo de la función humana, no como su sustituto.
- Garantizar interfaces comprensibles y seguras, adaptadas al nivel técnico de los usuarios finales.
- Documentar el funcionamiento general de los modelos utilizados, sus fuentes, limitaciones y sesgos conocidos.
- Implementar mecanismos sistemáticos para detectar y corregir errores.
- Evaluar regularmente el rendimiento del sistema, asegurando su conformidad con los principios éticos y legales.

Tratamiento de datos personales e información, sensible o confidencial

- Aplicar los principios y obligaciones establecidas en la normativa de protección de datos en aquellos casos de uso que impliquen tratamiento de datos personales: minimización, limitación de finalidad y proporcionalidad en el uso de datos personales, facilitar la ejecución de derechos y, en su caso, actualizar las Evaluaciones de Impacto en la Protección de Datos (EIPD) de los tratamientos cuando los sistemas IAG sufran modificaciones significativas.

- Implementar los casos de uso que traten información personal, sensible o confidencial preferentemente en sistemas Internos o en sistemas ad-hoc que garanticen el control de la organización.
- Establecer los mecanismos que sean necesarios para evitar que los usuarios introduzcan información personal, sensible o confidencial en sistemas no estén explícitamente autorizados para tratar dichos datos.
- Configurar los sistemas IA aplicando los principios de minimización y conservación limitada de datos en cuanto al acceso a datos de la organización, datos de usuario, metadatos y capacidad de memoria del sistema.
- Implementar mecanismos eficaces de validación y control humano en casos de uso que puedan implicar la toma de decisiones automatizadas basadas únicamente en el tratamiento automatizado que produzca efectos jurídicos o afecte significativamente a los derechos y libertades de las personas.
- Formar a los usuarios en técnicas eficaces para formular sus consultas a la IAG de forma clara y eficaz, evitando detalles específicos o irrelevantes que puedan comprometer la privacidad y confidencialidad de la información o los datos personales.

Transparencia y explicabilidad

- Garantizar la explicabilidad y transparencia de las decisiones automatizadas, si las hubiera, asegurando que sean comprensibles para los ciudadanos y permitan la rendición de cuentas.
- Asegurar que los sistemas IAG son transparentes con relación a las fuentes utilizadas y los criterios de selección o descarte.
- Documentar los procedimientos y decisiones relacionadas con el uso de la IAG en cada caso de uso.
- Implementar mecanismos de trazabilidad y registros de actividad que permitan verificar la lógica y el contexto de cada decisión basada en IAG.
- Hacer visible en los interfaces de aplicaciones corporativas en qué situaciones se está interactuando con una IA e incluir avisos de revisión humana obligatoria.

Seguridad y disponibilidad

- Someter los sistemas IAG a categorización conforme al Esquema Nacional de Seguridad (ENS) y aplicar controles según el nivel resultante.
- Implementar cifrado en tránsito y reposo, autenticación y control de acceso basado en roles.
- Garantizar el aislamiento de entornos críticos (sistemas que operen con información clasificada o de alto impacto) del resto de redes, especialmente de Internet.
- Establecer mecanismos de supervisión y respuesta ante incidentes de seguridad que incluyan la monitorización continua y gestión de incidentes.

- Desarrollar planes de continuidad y respaldo que aseguren la disponibilidad de los procesos clave, en particular, evitar dependencia de un único proveedor.
- Ajustar el uso de los sistemas IAG a las políticas corporativas de control de accesos.
- Evitar depender de la IAG en decisiones críticas o urgentes: No se debe confiar en estas herramientas para procesos que requieran máxima precisión, inmediatez o seguridad, ya que pueden ser inestables o poco fiables

Contratación

- Antes de contratar sistemas IAG evaluar el tratamiento de metadatos, logs y telemetría, el uso de datos para entrenamiento, para mejorar servicios o cualquier otra finalidad por parte del proveedor.
- Evaluar también la ubicación de los datos, periodos de retención, control de versiones y estabilidad contractual.
- De forma general, siempre que se opte por sistemas externos, garantizar la contratación de servicios en modalidad empresarial que garantice la gobernanza por parte de la organización.
- Incluir cláusulas de no reutilización de datos y de cumplimiento del RGPD, RIA y ENS en los contratos con proveedores.
- Verificar la existencia de mecanismos configurables en relación con ajustes de privacidad, que permita deshabilitar todas aquellas funcionalidades que puedan suponer una amenaza para los objetivos de privacidad y seguridad perseguidos por la organización.

Recursos humanos y capacitación

- Restringir el uso de sistemas IAG a usuarios formados y autorizados.
- Evaluar el impacto laboral de la IAG en el plan de supervisión (sobrecarga o redistribución de funciones).
- Garantizad la capacitación continua, formando regularmente a los usuarios.
- Establecer canales de comunicación bidireccional, con relación al uso de IAG en los procesos de la organización, entre los usuarios y los equipos de gestión, más allá de la gestión de incidentes.

Uso responsable de herramientas de IA generativa

- Desarrollar limitaciones de uso específicas para los sistemas de IAG que lo requieran y formar a los usuarios en esas limitaciones.
- Formar a los usuarios en las técnicas adecuadas para analizar críticamente cualquier respuesta generada por IA, permitiéndoles detectar errores o sesgos. Advertirles que no deben asumir que la información es correcta sin comprobarla.
- Informar explícitamente a los usuarios de:
  - La prohibición de utilizar sistemas IAG no registrados en el inventario corporativo.
  - La obligación de revisar y validar manualmente los resultados generados antes de su uso o publicación.

- La obligación de no compartir información confidencial, nunca ingresar datos privados, información no pública o datos personales.
- La obligación de respetar la propiedad intelectual e industrial.
- La prohibición de incluir el contenido generado por IAG en textos que produzcan efectos jurídicos, en resoluciones o en cualquier documento oficial sin revisión y validación humana.