POLÍTICA PARA EL DESARROLLO Y USO DE LA INTELIGENCIA ARTIFICIAL EN PROCESOS ADMINISTRATIVOS DE LA SUPERINTENDENCIA DE PROTECCIÓN DE DATOS PERSONALES

Elaborada por Luis Enríquez
Intendente General de Innovación Tecnológica y Seguridad de Datos Personales

30 de Diciembre de 2025

CONTENIDOS

1. INTRODUCCIÓN

La implementación de la Inteligencia Artificial (IA) en la administración pública trae beneficios y desafíos. Los beneficios de esta implementación deben reflejarse en la eficacia y la eficiencia de la gestión de trámites administrativos para la atención a los ciudadanos, y en la eficiencia de los procesos administrativos internos de la Superintendencia de Protección de Datos Personales (SPDP). Considerando que la SPDP tiene el deber de proteger los derechos y libertades de los titulares de datos personales, somos conscientes de nuestro desafío de desarrollar una inteligencia artificial confidencial y soberana, que este a la vanguardia del desarrollo tecnológico, y que a la vez, incorpore los principios de seguridad y protección de datos personales desde el diseño y por defecto en sus sistemas inteligentes.

Esta política general para el desarrollo y uso de la IA en los procesos administrativos es de uso interno, y se fundamenta en la gestión de riesgos de la IA, en las siguientes dimensiones: protección de datos personales, equidad, intervalo de acierto y robustez, explicabilidad y seguridad de la información. Es fundamental considerar que la implementación de la IA debe estar adaptada a las necesidades particulares de la SPDP. Esto quiere decir que es necesario utilizar nuestra propia ingeniería de contexto con el objeto de procesar información confidencial con controles de acceso, y entrenar sistemas de inteligencia artificial que se adapten a nuestras necesidades específicas. La ingeniería de contexto incorpora sets de datos para el entrenamiento, documentos confidenciales en un entorno confidencial de Retrieval-Augmented Generation (RAG), bases de datos vectoriales, y sistemas auxiliares de analítica predictiva en conformidad a la LOPDP, su reglamento, y la normativa secundaria de la SPDP. De igual manera, esta política establece las directrices generales sobre el uso de inteligencia artificial generativa para el trabajo de los funcionarios.

2. GOBERNANZA

La Inteligencia artificial presenta enormes ventajas cuando es incorporada de manera eficaz, eficiente, transparente y rentable en el sector público. En este contexto es necesario diferenciar entre la IA agéntica que es desarrollada y personalizada en la SPDP para cumplir con las finalidades sustantivas alineadas a nuestro estatuto de funcionamiento, y los usos de IA generativa que pueden realizar los funcionarios de la SPDP para cumplir con su trabajo tanto en el área sustantitiva, como en el área adjetiva.

2.1. Gobernanza de la IA agéntica. La Intendencia General de Innovación Tecnológica y Seguridad de Datos personales estará a cargo del diseño, desarrollo e implementación de agentes inteligentes y sistemas expertos basados en analítica predictiva, para cumplir con el compromiso de servir de manera eficaz y eficiente a la sociedad ecuatoriana. Los roles serán los siguientes:

Responsable Organizacional: El Superintendente de Protección de Datos Personales como máxima autoridad de la SPDP, será el responsable organizacional. Su función será aprobar las estrategias de desarrollo y de la implementación por parte del Responsable de la IA agéntica.

Responsable de la IA agéntica: El Intendente General de Innovación Tecnológica y seguridad de datos personales será el responsable de crear las estrategias, operaciones y tácticas para el desarrollo y la implementación de IA agéntica y sistemas expertos.

Responsable de desarrollo de IA agéntica. Un funcionario de la Intendencia General de Innovación Tecnológica nombrado por el Intendente General de Innovación Tecnológica y Seguridad de Datos

personales, será responsable del desarrollo de la inteligencia artificial agéntica, incluyendo protocolos, ingeniería de contexo, de modelos, y de sistemas expertos.

Responsable de seguridad de la IA agéntica. Un funcionario de la Intendencia General de Innovación Tecnológica nombrado por el Intendente General de Innovación Tecnológica y Seguridad de datos personales, será responsable de la seguridad de la IA agéntica. Esto incluye controles de acceso, verificación de integridad de sistemas de IA, y la disponiblidad de los servicios.

Oficial de Seguridad de la información (OSI). El OSI de la SPDP podrá verificar y auditar los sistemas de IA agéntica desarrollados e implementados por la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales. El OSI deberá considerar estos sistemas inteligentes dentro de su gestión de seguridad organizacional, tales como la identificación de activos, gestión de riesgos, declaración de aplicabilidad, entre otros relacionados a su gestión.

Delegado de Protección de Datos (DPD). El DPD de la SPDP podrá verificar y auditar los sistemas de IA agéntica desarrollados e implementados por la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales. El DPD podrá consultar al equipo desarrollador e implementador acerca de la implementación de medidas de seguridad organizacionales y técnicas, tales como la implementación de tácticas de privacidad diferencial, controles de acceso, minimización de datos, y todo lo concerniente para la protección de los derechos y libertades de los titulares de datos personales.

2.2. Gobernanza de la IA generativa. La Unidad no jerarquizada de planificación y gestión estratégica será la encargada de gobernar el uso de IA generativa para lo cual recomendará el establecimiento de procesos institucionales al Responsable Organizacional.

Responsable Organizacional: El Superintendente de Protección de Datos Personales como máxima autoridad de la SPDP, será el responsable organizacional. Su función será aprobar los procesos institucionales recomendados por la Unidad no jerarquizada de planificación y gestión estratégica.

Responsable de procesos de IA generativa. El Analista de procesos será el responsible del apoyo metodológico para la utilización de aplicativos fundamentados en IA generativa.

Responsable de planificación y gestión estratégica. El Especialista de planificación y gestión estratégica será el responsible de revisar la conveniencia de la utilización de la IA generativa para diferentes tareas adjetivas de la institución.

Responsables funcionales de cada Unidad. El funcionario de mayor rango de cada Unidad controlará el uso responsable de IA generativa por parte de los funcionarios a su cargo. De igual manera, se comunicará con el responsable de procesos de IA generativa cuando sea necesario crear un nuevo proceso que utilice IA generativa, y se comunicará con el Responsable de planificación y gestión estratégica cuando sea necesario analizar la conveniencia acerca del uso de IA generativa en procesos institucionales.

Oficial de Seguridad de la información. El OSI de la SPDP podrá verificar y auditar la seguridad de los procesos que utilicen IA generativa en la SPDP. El OSI deberá considerar estos procesos dentro de su gestión de seguridad organizacional, tales como la identificación de activos, gestión de riesgos, declaración de aplicabilidad, entre otros relacionados a su gestión.

Delegado de Protección de Datos. El DPD de la SPDP podrá verificar y auditar los procesos que utilicen IA generativa, y que involcren, o pudiesen involucrar el tratamiento de datos personales. El PDP podrá asesorar y auditar la implementación de estrategias, operaciones y tácticas de privacidad diferencial, controles de acceso, minimización de datos, y todo lo concerniente para la protección de los derechos y libertades de los titulares de datos personales.

3. OBJETIVOS

-Productividad.- Incrementar la productividad en los trámites ciudadanos tales como notificaciones, solicitudes y denuncias.

- Eficiencia. Ser eficaces y eficientes en los procedimientos administrativos internos, y a la vez, obtener un retorno a la inversión en relación al costo de implementar IA, y sus beneficios.

- Escalabilidad. Controlar la capacidad de la SPDP para manejar la demanda creciente de trámites ciudadanos y procesos administrativos en el mediano y largo plazo.

- Confidencialidad. Proteger la confidencialidad de la información en un entorno de desarrollo y de producción con estrictos controles de acceso y tecnologías para el mejoramiento de la privacidad (PET).

- Seguridad. Realizar auditorías de vulnerabilidades, perfilamiento de amenazas, y pruebas de stress y de penetration testing permanentes.

- Soberanía tecnológica. Desarrollar analítica predictiva, entrenamiento de sistemas de IA con modelos de aprendizaje automático y de aprendizaje profundo en servidores y nubes confidenciales de la SPDP. Se podrán utilizar Modelos de IA de terceros siempre y cuando cumplan con lo establecido en la sección de gestión de riesgos de esta política.

- Trazabilidad y explicabilidad. El desarrollo de sistemas expertos basados en IA serán trazables y explicables. Esto es posible cuando los pesos decisionales y analíticos de los modelos de IA son desarrollados por la propia SPDP.

- Gestión de riesgos. El enfoque de gestión de riesgos consiste en reducir la incertidumbre para una toma de decisiones informada. Por ello, nuestros sistemas inteligentes serán de asistencia al humano para la toma informada de decisiones, y para sustentar cualquier decision de manera objetiva.

4. ACTIVIDADES EN LAS QUE SE PUEDE UTILIZAR IA AGÉNTICA

- Notificaciones de vulneración de la seguridad de datos personales. Se utilizarán agentes inteligentes proactivos para recuperar datos de notificaciones de vulneraciones de la seguridad de datos personales, con los fines de: obtener la trazabilidad de cada expediente, comprender el *rationale* que sustenta una decisión, realizar estadística y analítica de datos. Se desarrollarán métricas significativas y modelos adecuados de riesgo que permitan informar a los funcionarios competentes acerca de los factores a considerar para establecer el nivel de riesgo que cada incidente de seguridad haya tenido, tenga, o pudiese tener en el futuro, y que pudiese vulnerar los derechos y libertades de los titulares de datos personales. Los agentes inteligentes contarán con supervisión humana en todas sus instancias.

- Procesamiento de denuncias y solicitudes. Se utilizarán agentes inteligentes proactivos para tramitar denuncias y solicitudes ciudadanas, con el objeto de obtener la trazabilidad de cada expediente, realizar estadística y analítica de datos. Se generarán métricas significativas y modelos adecuados de riesgo que permitan informar a los funcionarios acerca de los factores a considerar para establecer el nivel de riesgo contra los derechos y libertades de los titulares de datos personales en cada caso, con la finalidad de que los funcionarios puedan tomar decisiones informadas y objetivas. Los agentes inteligentes contarán con supervisión humana en todas sus instancias.

- Interacción entre agentes inteligentes. Se construirán protocolos para la interacción entre agentes inteligentes, que puedan orientar de manera adecuada la resolución de controversias y conflictos en función de informar los probables riesgos de cada caso en particular.

- Sistemas de alertas de incidentes de seguridad de la información. Se desarrollarán herramientas de analítica predictiva para la creación de sistemas de alarmas y detección de anomalías que permitan a los funcionarios competentes vigilar la seguridad de los activos y de los procesos institucionales de la SPDP de manera proactiva.

- Chatbots para ayuda a los ciudadanos en las plataformas digitales de la SPDP. Se desarrollarán también chatbots para asesorar y ayudar a los ciudadanos a realizar sus trámites en el Sistema Nacional de Protección de Datos Personales SISPDP.

5. ACTIVIDADES QUE SE PUEDE UTILIZAR IA GENERATIVA

- Gestión de archivos de texto. Se podrán utilizar aplicaciones y sistemas entrenados con IA gestionados por terceros, para extraer, analizar, traducir y generar información con respecto a procesos administrativos no confidenciales, y que no contengan datos personales. Para los procesos calificados como confidenciales o que involucren el tratamiento de datos personales, deberá cumplirse con lo establecido en el capítulo sobre gestión de riesgos.

- Gestión de contenidos multimedia. Se podrá utilizar inteligencia artificial generativa para desarrollar cualquier contenido multimedia, siempre y cuando no se compartan datos personales en aplicaciones de terceros. Para los procesos calificados como confidenciales o que involucren el tratamiento de datos personales, deberá cumplirse con lo establecido en el capítulo sobre gestión de riesgos.

- Asistencia en consultas y tareas de desarrollo. Se podrá utilizar Ia generativa para realizar consultas legales, jurídicas, doctrinarias, y cualquiera de propósito legal. Se podrán utilizar agentes inteligentes personalizados para generación de texto y de código en lenguajes de programación bajo estricta supervisión humana, siempre y cuando siempre y cuando no se suban ni compartan datos personales en aplicaciones de terceros.

6. GESTIÓN DE RIESGOS DE LA IA AGÉNTICA

- Protección de datos personales. Es obligatorio implementar los principios establecidos en la guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales, y seguir las etapas establecidas para la gestión de riesgos establecidas en las normas ISO 31000 e ISO/IEC 27005. Además se implementarán las estrategias, operaciones y tácticas establecidas en la guía de protección de datos desde el diseño y por defecto, cuando sean necesarias y aplicables. Se realizará una gestión de riesgos proactiva y periódica, para la protección de derechos y libertades en dos ejes: datos de entrada

y datos de salida. Para los datos de entrada utilizados para el entrenamiento de los sistemas inteligentes, se implementarán medidas de privacidad diferencial que disocien cualquier indicio de identidad de los titulares de los datos en un nivel adecuado de aceptación al riesgo. Los datos personales y otra información confidencial, serán gestionados en entornos confidenciales de tipo Retrieval-Augmented Generation con bases de datos vectoriales gobernadas por la SPDP, con estrictos controles de acceso y en servidores o nubes confidenciales de la SPDP.

Para los datos de salida, se desarrollará código en lenguajes de programación con el fin de filtrar, masquear, obfuscar datos personales en la interacción entre el prompt y el funcionario.

- Equidad. Es necesario identificar sesgos discriminatorios que pueden ser inherentes en los sets de datos utilizados para entrenar modelos de IA. Se comprenderán como sesgos discriminatorios aquellos que discriminen a una persona por razones de género, etnia, nacionalidad, edad, salud. Para identificarlos, se implementarán métricas de equidad tales como *average odds difference, equal oportunity difference, disparate impact, demographic parity, statistical parity difference*, entre otras.

Se implementarán medidas de tratamiento de riesgos para calibrar el nivel de vulnerabilidad de las personas naturales, con el fin de contar con agentes inteligentes neutrales.

- Intervalo de acierto y robustez. Los modelos de analítica predictiva e inteligencia artificial desarrollados o personalizados por la SPDP deberán cumplir un nivel de acierto aceptable en términos de eficacia y eficiencia, y siempre será superior a una hipótesis nula. Los modelos deberán cumplir con niveles aceptables de robustez en contra de errores del modelo, alucinaciones, o de ataques internos o externos que puedan vulnerar la integridad y respuesta de los sistemas de IA agéntica.

- Explicabilidad. Las respuestas que generan nuestros sistema de IA agéntica constituyen datos informativos para la toma de decisiones por parte de los funcionarios. Las métricas y modelos de riesgo desarrollados por la Intendencia General de Innovación Tecnológica y Seguridad de Datos Personales implementados en nuestros propios RAGs, nos permiten sustentar cualquier insumo informativo que sirva para sustentar las decisiones de nuestros funcionarios.

- Seguridad de la información. La confidencialidad, integridad y disponibilidad de los agentes inteligentes deberá ser protegida con medidas organizacionales y técnicas de seguridad de la información. Para ello, se seguirán varias guías como la norma ISO/IEC 27001, la ISO/IEC 42001, el OWASP Top Ten for LLMs, el OWASP Top Ten para aplicaciones agénticas, y otras normas de relevancia en la industria.

7. GESTIÓN DE RIESGOS DE LA IA GENERATIVA

- Protección de datos personales. Es obligatorio implementar los principios establecidos en la guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales, y seguir las etapas establecidas para la gestión de riesgos establecidas en las normas ISO 31000 e ISO/IEC 27005. Además se implementarán las estrategias, operaciones y tácticas establecidas en la guía de protección de datos desde el diseño y por defecto, cuando sean necesarias y aplicables. No se podrá bajo ninguna causal subirse datos personales en chatbots que utilicen modelos de IA en aplicaciones de terceros tales como ChatGPT (Open IA), Gemini (Google), Llama (Meta), Grok(X), y similares, a menos que se cuente con el consentimiento de los titulares de los datos. Es obligatorio eliminar u obfuscar los datos personales antes de subirlas a estos aplicativos de terceros. De no ser posible la eliminación, es necesaria la anonimización de datos personales antes de subirlos a los aplicativos mencionados.

- Equidad. No se podrá utilizar IA generativa para sustentar cualquier decisión discriminatoria por razones de género, etnia, nacionalidad, edad, salud, y similares.

- Intervalo de acierto y robustez. Es fundamental considerar que los aplicativos de IA de terceros no son 100% confiables, pues pueden tener alucinaciones y errores en los datos que dan como respuesta. Todo funcionario deberá verificar cualquier tipo de información obtenida mediante aplicativos de IA generativa. Es necesario que los funcionarios aprendan técnicas esenciales para el prompting, como la utilización formatos JSON.

- Explicabilidad. Es necesario utilizar técnicas de Cadena de pensamiento (Chain of Thought) para entender el razonamiento de un sistema de IA generativa para llegar a una respuesta. Será preferible utilizar los modelos de IA de peso abierto (open weight). No obstante, la IA generativa será utilizada como herramienta auxiliar para comprender un problema y para la gestión de archivos de texto y multimedia. No se utilizará IA generativa de terceros para la creación de métricas y establecimiento de pesos en los procesos administrativos confidenciales.

- Seguridad de la información. Los funcionarios que utilicen IA generativa deberán informar a la Dirección de planificación y al Oficial de Seguridad de la información procesos acerca de la manera como la utilizan. Estos aprobarán el uso de IA generativa de acuerdo al tipo de actividad a desarrollarse y al nivel de riesgo que esta conlleve en relación al tipo de información, y a la capacidad individual y conocimientos en seguridad de la información del funcionario que la utilice.

8. CONCLUSIÓN

Esta política tiene la finalidad de mejorar a gestión interna y externa de la SPDP, utilizando IA agéntica e IA generativa. Para la IA agéntica, se incentiva el desarrollo de agentes inteligentes que ayuden a mejorar la productividad y eficiencia organizacional, además de contribuir con los datos, métricas y modelos de riesgo adecuados para una toma de decisiones informada por parte de los funcionarios. Para la IA generativa, se abre la posibilidad de utilizar aplicativos de IA generativa de terceros siempre y cuando se cumpla con medidas fundamentales de gestión de riesgos para proteger de manera adecuada la confidencialidad de la información, y los derechos y libertades de los titulares de datos personales.

9. DISPOSICIONES TRANSITORIAS

Esta política será revisada y actualizada anualmente por defecto, o cuando así lo requiera el responsable organizacional.