Facultad de Ciencias Jurídicas, Políticas y Relaciones Internacionales

Especialización en Cumplimiento y Anticorrupción

Tema:

Política de Protección de Datos Personales para el Uso Ético de un Sistema Ia

Trabajo de Titulación para la obtención del Título de

Especialista en Cumplimiento y Anticorrupción

Presentada por:

Daniel Fernando Mejía Terán

Gabriel Omar Macas Ramírez

Fernando Alonso Palacios Navas

Tutor:

Diego Mauricio Álvarez Mejía

Quito, julio de 2024

Resumen

Nuestra propuesta consiste en una Política Corporativa con enfoque hacia la protección de datos personales en aquellos casos que se utilice o se pretenda utilizar un sistema de inteligencia artificial para el tratamiento de datos personales. La Política prevé buenas prácticas en protección de datos personales según la Ley Orgánica de Protección de Datos Personales del Ecuador, y su Reglamento. Adicionalmente, posee un marco conceptual basado en el Reglamento de la Unión Europea para el uso de Inteligencia Artificial.

Palabras clave: Protección de Datos Personales, Inteligencia Artificial, Organización

Abstract

Our proposal consists of a Corporate Policy focused on the protection of personal data in cases where an artificial intelligence system is used or intended to be used for the processing of personal data. The Policy provides best practices in personal data protection according to the Organic Law on Personal Data Protection of Ecuador and its Regulations. Additionally, it has a conceptual framework based on the European Union Regulation for the use of Artificial Intelligence.

Keywords: Personal Data Protection, Artificial Intelligence, Organization

Declaración de aceptación de norma ética y derechos

El presente documento se ciñe a las normas éticas y reglamentarias de la Universidad Hemisferios. Así, declaro que lo contenido en este ha sido redactado con entera sujeción al respeto de los derechos de autor, citando adecuadamente las fuentes. Para la elaboración del presente trabajo se han podido utilizar datos confidenciales de una o más organizaciones por lo que se adjunta el correspondiente acuerdo de confidencialidad.

De comprobarse que no cumplí con las estipulaciones éticas, incurriendo en caso de plagio, me someto a las determinaciones que la propia Universidad plantee.

Fernando Alonso Palacios Navas

C.C.1750738336

Declaración de aceptación de norma ética y derechos

El presente documento se ciñe a las normas éticas y reglamentarias de la Universidad Hemisferios. Así, declaro que lo contenido en este ha sido redactado con entera sujeción al respeto de los derechos de autor, citando adecuadamente las fuentes. Para la elaboración del presente trabajo se han podido utilizar datos confidenciales de una o más organizaciones por lo que se adjunta el correspondiente acuerdo de confidencialidad.

De comprobarse que no cumplí con las estipulaciones éticas, incurriendo en caso de plagio, me someto a las determinaciones que la propia Universidad plantee.

Daniel Fernando Mejía Terán

C.C.1727420141

Declaración de aceptación de norma ética y derechos

El presente documento se ciñe a las normas éticas y reglamentarias de la Universidad Hemisferios. Así, declaro que lo contenido en este ha sido redactado con entera sujeción al respeto de los derechos de autor, citando adecuadamente las fuentes. Para la elaboración del presente trabajo se han podido utilizar datos confidenciales de una o más organizaciones por lo que se adjunta el correspondiente acuerdo de confidencialidad.

De comprobarse que no cumplí con las estipulaciones éticas, incurriendo en caso de plagio, me someto a las determinaciones que la propia Universidad plantee.

Gabriel Omar Macas Ramírez

C.C. 1724013030

Índice De Documentos

El índice de documentos enlista todos los elaborados incluyendo matrices, encuestas, instructivos, políticas, etc. Y contiene una breve explicación (máx. 200 palabras de cada uno)

1.1.Contexto y justificación

En el año 2017 se transformó la cosmovisión empresarial y legal, con la adopción de una nueva premisa global: “El recurso más valioso del mundo ya no es el petróleo, sino los datos” (The Economist, 2017). Precisamente por esta premisa, resulta necesario las buenas prácticas en protección de datos personales para las Organizaciones empresariales cuyo giro de negocio involucre el tratamiento de datos personales de clientes, consumidores o proveedores.

Adicionalmente, en la actualidad ha emergido un nuevo actor al escenario de la globalización y liquidez de la sociedad: la Inteligencia Artificial (IA). Al respecto, este nuevo concepto plantea muchos cuestionamientos sobre su uso, específicamente, discusiones en torno a la ética en la utilización de nuevas tecnologías. La Comisión de la Unión Europea ha planteado que uno de los principios para alcanzar la ética en el uso de la Inteligencia Artificial es la protección y privacidad de los datos personales (Parlamento de la Unión Europea , 2024).

Por todo lo expuesto, resulta justificable la presentación de una Política Corporativa de Protección de Datos Personales para el uso ético de un Sistema IA.

1.2.Objetivo principal de la Política

El objetivo principal de la Política es implementar prácticas de protección de datos personales para una Organización Empresarial que trate datos personales como factor inherente a su giro de negocio, a través de un sistema de Inteligencia Artificial, y evitar

sanciones por la Autoridad de Protección de Datos Personales, o en un futuro no muy lejano, una Autoridad de Inteligencia Artificial.

1.3.Alcance de la Política

La Política tiene un ámbito de alcance para aquellas Organziaciones Empresariales Nacionales (Ecuador) que tratante datos personales y para aquellas Organizaciones Empresariales Internacionales que traten datos personales de ecuatorianos, con sistemas de Inteligencia Artificial. Asimismo, la Política tiene dos dimensiones: 1. Preventiva / Proactiva, 2. Reactiva. La primera dimensión hace referencia a una actuación previa y sin la necesidad de ser sancionada, para empezar un proceso de cumplimiento de buenas prácticas en protección de datos personales y uso ético de sistemas IA.

Por otro lado, la segunda dimensión consiste en la viabilidad práctica de la Política a través de mecanismos de protección directa hacia los titulares de los datos personales tratados por la Organización Empresarial.

2. Beneficios de la Política

Existen tres beneficios de la Política: 1. Educación Organizacional, 2. Innovación Segura, 3. Ética Empresarial. Sobre el primer beneficio, la Política permite que se construya una cultura organizacional basada en protección de datos personales y ética digital. El segundo beneficio trata el incentivo hacia las Organizaciones Empresariales para la innovación segura a través del uso de una Política de Protección de Datos Personales aplicable a tratamientos con sistemas de Inteligencia Artificial (factor innovador). Finalmente, el tercer beneficio consiste en promover la ética empresarial a través de una cultura organizacional de cumplimiento espontáneo en protección de datos personales y compromiso con los principios de la ética digital.

2.1. Ética Digital

La Política propone un decálogo de principios para afianzar la ética digital como un compromiso adquirido por la Organización para implementar la Política. Los principios que se promueven son: transparencia en la recolección de datos personales, consentimiento informado, minimización de datos personales, seguridad de los datos, derechos de acceso, rectificación, eliminación, oposición, etc., uso ético de la Inteligencia Artificial, equidad y no discriminación, innovación responsable, capacitación continua, cumplimiento normativo (Instituto Nacional de Transparencia, Acceso a la información y Protección De Datos Personales, 2022).

2.2.Modelos de Inteligencia Artificial

Existe bastante desinformación sobre las definiciones y tipologías de la Inteligencia Artificial, además de una asimetría de información en el mercado de proveedores de sistemas IA, que está perjudicando al desarrollo correcto y ético de dichas tecnologías. En ese sentido, la Política hace énfasis en su marco conceptual, empezando por la descripción de los tipos de modelos de Inteligencia Artificial, que son los siguientes:

A. Red Neuronal Artificial: Campo de la informática que desarrolla sistemas y algoritmos que realizan tareas cognitivas como el reconocimiento de patrones, la toma de decisiones y el aprendizaje automático (Instituto Nacional de Transparencia, Acceso a la información y Protección De Datos Personales, 2022).

B. Inteligencia Artificial General (AGI): Capacidad de entender, aprender y aplicar conocimientos de manera similar a los humanos en amplia variedad de tareas (Instituto Nacional de Transparencia, Acceso a la información y Protección De Datos Personales, 2022).

C. Aprendizaje Automatizado: Las técnicas a comprenderse son el Machine Learning y Deep Learning (Instituto Nacional de Transparencia, Acceso a la información y Protección De Datos Personales, 2022).

D. Automatización robótica de procesos (RPA): Se incluye el manejo de Big Data en diferentes tipologías de procedimientos y necesidades de una organización (Instituto Nacional de Transparencia, Acceso a la información y Protección De Datos Personales, 2022).

2.3. Funciones de la Inteligencia Artificial

Al igual que el acápite anterior, la Política profundiza el marco conceptual de la Inteligencia Artificial, y se desarrollan sus tipologías según el funcionamiento específica de la IA:

a. Máquinas reactivas: Son máquinas que tienen la capacidad de analizar situaciones y responder a ellas en tiempo real, un tipo básico de inteligencia artificial basado en decisiones del presente. No tienen memoria ni capacidad de usar experiencias pasadas para evolucionar o tomar decisiones futuras.

b. Memoria limitada: Utilizan experiencias previas, tienen memoria y pueden aprender de datos históricos propios o transmitidos, por ello es utilizada en la toma de decisiones actuales.

c. Teoría de la mente: Son capaces de comprender y replicar pensamientos, emociones e ideas, evalúan procesos de razonamiento y de conducta. Se incluyen capacidades de trabajo en equipo con seres humanos ejecutando estrategias en procesos mentales acorde a la percepción obtenida. Está en línea con comportamientos, patrones y normas sociales en objetivos de interacción.

d. Autoconciencia: Se prevé que tendrá una forma de conciencia similar a la humana, dotando a las máquinas de facultades de autoconciencia, se pudiesen representar a sí mismas, a su entorno y tendría sentimientos externos de acuerdo a la percepción, el conocimiento adquirido, experiencias y la subjetiva valoración de la información.

2.4.Sistemas IA de Alto Riesgo

Los Sistemas IA de Alto Riesgo poseen dicha categoría debido al grado de afectación de derechos que pueden generar en su uso. La Política ofrece una clasificación de los tipos de actividades o tratamiento de datos personales que procesados por un sistema IA, se consideren de alto riesgo. Al respecto, los ámbitos donde se desarrollan esta clase de sistemas IA, son (Parlamento de la Unión Europea , 2024):

A. Tratamiento de Datos Biométricos.

B. Infraestructuras para el suministro de servicios básicos.

C. Educación y formación profesional.

D. Gestión de empleo y autoempleo.

E. Gestión de nómina.

F. Gestión judicial por Autoridades Públicas.

G. Gestión y control migratorio.

H. Procesos de participación electoral.

2.5.Principios para el uso ético de la IA y principios para la protección de datos personales

Nuevamente, la Política busca consolidar una cultura organizacional a través del compromiso de cumplir y acatar con los principios para un uso ético de la Inteligencia Artificial y los principios de protección de datos personales.

La primera clasificación de principios son mandatos de optimización para la Organización empresarial, y por otro lado, la segunda clasificación son reglas de cumplimiento en protección de datos personales de exigibilidad para la Organización Empresarial.

La primera clasificación prevé principios cómo: Protección de datos personales y privacidad, transparencia, no discriminación, responsabilidad, seguridad de la información (Instituto Nacional de Transparencia, Acceso a la información y Protección De Datos Personales, 2022).

Por otro lado, la segunda clasificación prevé principios como: legalidad, transparencia, finalidad, pertinencia y minimización, proporcionalidad, confidencialidad, etc. (Asamblea Nacional del Ecuador, 2021).

2.6.Bases de legitimación para el tratamiento de datos personales

La Política describe cada una de las bases de legitimación para el tratamiento de datos personales, exhortando su interpretación como requisitos para la Organización Empresarial que debe legalizar y legitimar los tratamientos de datos personales que éste ejecutando. Las bases de legitimación son las siguientes Consentimiento, obligación legal, obligación contractual y pre contractual, mandato judicial. misión de interés público, intereses vitales, fuentes de información de acceso público, interés legítimo (Asamblea Nacional del Ecuador, 2021).

2.7.Ciclo de vida del dato personal y el sistema de protección de datos personales

El ciclo de vida del dato personales es un conjunto de cinco fases: 1. Captura, 2. Almacenamiento, 3. Procesamiento, 4. Transferencia / Comunicación, 5. Destrucción. Esta es la metodología que plantea la Política para que la Organización pueda identificar sus tratamientos de datos personales.

En contraste, la Política describe la interacción de los actores del sistema nacional de Protección de Datos Personales, con el objetivo de trazar e identificar el flujo de actuación de un titular de los datos y sus demás actores: Responsable, Encargado, Destinatario, Delegado, Autoridad de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021).

2.8.Tratamientos de datos personales con sistemas IA y los roles de Responsable y Encargado del Tratamiento

La concatenación de la protección de datos personales y el uso de sistemas de inteligencia artificial es a través de la identificación de los tipos de tratamientos de datos personales que puede realizar un sistema IA, y los roles de Responsable y Encargado, según cada tratamiento. Al respecto, los tipos de tratamientos son:

a. Entrenamiento: Se podrían utilizar datos personales en el desarrollo de este. En otras ocasiones, como es el caso en el que se entrene un modelo IA mediante la captura de conocimiento de un experto, podría considerarse a priori que no existe un tratamiento de datos de carácter personal (Agencia Española de Protección de Datos Personales , 2020).

b. Validación: En esta operación se podría realizar un tratamiento de datos personales cuando se utilice datos que corresponden a la situación real del

tratamiento, para determinar la bondad del modelo de forma experimental (Agencia Española de Protección de Datos Personales , 2020).

c. Despliegue: En el caso que la solución IA sea un componente y/o un módulo que se distribuye a terceros para incluir en sus tratamientos, se considera que hay una comunicación de datos personales cuando se incluya datos personales o exista forma de obtenerlos (Agencia Española de Protección de Datos Personales , 2020).

d. Retirada: La retirada del servicio puede tener dos extensiones distintas: el componente IA se retira por obsoleto en todos los tratamientos en los que se implemente, o un usuario concreto decide no utilizar el componente IA. Ese usuario puede ser una entidad o una persona física y puede tener efectos en la supresión local, centralizada o distribuida de datos, así como sobre la portabilidad del servicio (Agencia Española de Protección de Datos Personales , 2020).

e. Explotación: En las distintas actividades de explotación de la solución IA es posible encontrar los siguientes tratamientos de datos personales (Agencia Española de Protección de Datos Personales , 2020):

Inferencia: cuando se usen datos del interesado para obtener un resultado, cuando se usen datos de terceros con el mismo propósito o cuando datos e inferencias del interesado se almacenan. Si el propio interesado dispone de la IA como un componente de su propiedad, aplicaría la excepción doméstica.

Decisión: como se ha visto anteriormente, la decisión sobre un interesado es un tratamiento de datos personales.

Evolución: en la solución IA se podrían usar los datos y resultados de los interesados para refinar el modelo de IA. Cuando nos encontramos que esa evolución se realiza en el componente adquirido por el propio interesado, de forma aislada y autónoma, aplicaría la excepción doméstica. Pero si se envían a terceros, tendríamos una comunicación de datos, un posible tratamiento de almacenamiento, tratamiento para modificar el modelo, o incluso nuevas comunicaciones si esos datos se incorporan al modelo y este es accesible a otros terceros.

2.9.Notificaciones de vulnerabilidades y atención de derechos

La Política viabiliza su implementación a través de los mecanismos de notificación de vulnerabilidades y de atención de derechos hacia los titulares, debido a que, es una de las formas idóneas de materializar el compromiso de protección de datos personales y uso ético de sistemas IA.

La notificación de vulnerabilidades consiste en un proceso de reportar los incidentes en seguridad de la información y seguridad de los datos personales (Asamblea Nacional del Ecuador, 2021).

La atención de derechos conexos a la protección de datos personales es una obligación determina en la Ley, para precautelar de forma directa las necesidades del titular de los datos personales en torno al ejercicio de sus derechos (Asamblea Nacional del Ecuador, 2021).

3. Anexos

Los anexos son insumos que ofrece la Política para realizar un diagnóstico de cumplimiento en protección de datos personales y uso ético de sistemas IA de la

Organización Empresarial. A partir de los resultados obtenidos de los anexos, la empresa podrá desarrollar un análisis de riesgos y evaluación de impacto, además de, diseñar un plan de acción para subsanar las brechas detectadas.

Referencias

Instituto Nacional de Transparencia, Acceso a la información y Protección De Datos Personales. (2022). *Recomendaciones para el tratamiento de datos personales derivados del uso de la Inteligencia Artificial.* México: Instituto Nacional de Transparencia, Acceso a la información y Protección De Datos Personales.

Agencia Española de Protección de Datos Personales . (2020). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción.* Madrid: Agencia Española de Protección de Datos Personales .

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales* (Vol. Registro oficial 459). Quito, Ecuador .

Parlamento de la Unión Europea . (2024). *Reglamento de Inteligencia Artificial* . Bruselas : Parlamento de la Unión Europea .

The Economist. (06 de mayo de 2017). *The Economist*. Obtenido de The world's most valuable resource is no longer oil, but data: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data