

## ÍNDICE

### **CAPÍTULO 1.- LA ECONOMÍA DE LOS DATOS DESDE EL PUNTO DE VISTA JURÍDICO: PRINCIPIOS PARA LA GESTIÓN Y GOBERNANZA DE DATOS**

#### 1. LA ECONOMÍA DEL DATO

- 1.1. El dataísmo
- 1.2. Ecosistemas y soluciones basadas en datos.
- 1.3. Monetización como estrategia de nuevo modelo de negocio
- 1.3. La Propiedad Intelectual del dato. Las bases de datos

#### 2. TIPOS DE BASES DE DATOS

- 2.1. Bases de datos relacionales (RDBMS)
- 2.2. Bases de datos NoSQL
- 2.3. Bases de datos de objetos

#### 3. DISEÑO, ESTRUCTURA Y GESTIÓN DE BASES DE DATOS

- 3.1. Creación y administración de bases de datos
- 3.2. La importancia del “privacy by design”
- 3.3. Aplicación de la técnica K-anonimización sobre las bases de datos relacionales
- 3.4. Aplicación de la técnica KitPriv: Toolkit de anonimización en las bases de datos relacionales
- 3.5. La Evaluación de Impacto de Protección de Datos (EIPD) para bases de datos: Interpretaciones
- 3.6. Derechos de los interesados en la bases de datos. El derecho al olvido en modelos de lenguaje grandes (LLM) GPT3 o GPT4
- 3.7. Bases de datos y cloud computing: Homologación de proveedores cloud
- 3.8. Tendencias en seguridad de almacenamiento cloud

### **CAPÍTULO 2.- DISEÑO DE ESTRATEGIAS PARA LA GOBERNANZA DEL DATO**

- 1. PASOS GENERALES EN EL PROCESO DE GOBERNANZA DE DATOS
- 2. PERSONAL IMPLICADO EN LOS PROCESOS DE GOBERNANZA DE DATOS Y GESTIÓN DE USUARIOS Y PERMISOS
- 3. GESTIÓN DE USUARIOS Y PERMISOS
- 4. LA GOBERNANZA Y CUMPLIMIENTO NORMATIVO EN PROTECCIÓN DE DATOS PERSONALES
- 5. TIPOLOGÍA DE DATOS

## **CAPÍTULO 3.- GOBERNANZA DE DATOS EN EL SECTOR PRIVADO Y PÚBLICO**

### **1. GOBERNANZA DE DATOS EN EL SECTOR PRIVADO**

- 1.1 La gobernanza de datos y la industrialización
- 1.2. Desafíos abordados por una gobernanza de datos eficaz
- 1.3. El Data Sharing Agreement (DSA) y herramientas de data governance
- 1.4. Ciclo de vida proyecto de análisis de datos y gobernanza de datos: preparación de datos y anonimización
- 1.5. Estudio de Clearview. Implicaciones jurídico-éticas en torno a la gobernanza de datos

### **2. GOBERNANZA DE DATOS EN EL SECTOR PÚBLICO**

- 2.1 La gobernanza de datos en el Sector Público. Errores frecuentes
- 2.2. La calidad de los datos y la limpieza. Ejemplos y buenas prácticas
- 2.3. Los datos de las Administraciones Públicas y las Comunidades Autónomas en España
- 2.4. Los datos abiertos
- 2.5. La Oficina del dato y la gobernanza de los datos

## **CAPÍTULO 4.- RIESGOS ÉTICOS EN EL TRATAMIENTO Y LA GESTIÓN DEL DATO: LA ÉTICA DE LOS DATOS**

### **1. ÉTICA, MORAL Y DERECHO EN LA ERA DIGITAL**

### **2. ÉTICA DE LOS DATOS EN EL SECTOR PRIVADO**

- 2.1. La ética impuesta. Los códigos de conducta. Canal de denuncias
- 2.1.1. Los comités de ética
- 2.1.2. La autoevaluación
- 2.1.3. Certificaciones y sellos de calidad de ética de los datos.
- 2.1.4. Ética desde el diseño
- 2.1.5. Privacidad como valor

### **3. ÉTICA DE DATOS EN EL SECTOR PÚBLICO**

- 3.1. Una mirada puesta en el sector salud: Tiempos de Covid-19
- 3.2. Vulnerabilidades de seguridad en hospitales y dispositivos

## **CAPÍTULO 5.- RIESGOS ÉTICOS EN EL TRATAMIENTO Y LA GESTIÓN DEL DATO EN IA**

### **1. UNA MIRADA A LA REGULACIÓN EN MATERIA DE IA**

- 1.1. Antecedentes regulatorios
- 2.2. El Reglamento General de protección de datos y su impacto (RGPD).
- 2.3. El Reglamento Europeo de IA y su impacto

1.3. La normativa en materia de responsabilidad de IA.

1.3.1. La Directiva (UE) 2024/2853 productos defectuosos o PLD.

1.3.2. Directiva sobre Responsabilidad Civil en materia de IA.

1.4. Otras normativas de interés: DSA, DMA Y DFA y su impacto.

## 2. RIESGOS ÉTICOS DEL DATO: OPACIDAD BLACK BOX Y DISCRIMINACIÓN ALGORÍTMICA.

2.1. Definición de opacidad y tipos

2.2. Dependencia algorítmica y necesidad de límites

2.3. Causas del sesgo discriminatorio

2.4. Las propiedades de los algoritmos

2.4.1. La “no neutralidad” de los algoritmos y transparencia de la IA

2.4.2. La reformulación de algoritmos como solución y la desidentificación insuficiente

2.5. ¿Son evitables los sesgos algorítmicos?

2.6. Casos de estudio: Caso Compas e Impact

## 3. GUÍA DE DIRECTRICES, REQUISITOS Y MÉTODOS TÉCNICOS PARA DESARROLLADORES DE IA

3.1. Requisitos ético-legales para desarrolladores en una IA confiable.

3.1.1. Respeto a la Agencia humana y supervisión

3.1.2. Respeto a la robustez técnica y seguridad

3.1.3. Respeto a la Privacidad y gobierno de datos

3.1.4. Respeto al gobierno de datos

3.1.5. Respeto a la transparencia

3.1.6. Respeto al Bienestar social y ambiental

3.1.7. Respeto a la Responsabilidad

3.2. Métodos técnicos y no técnicos para IA confiable

## 4. LA PARTICULARIDAD EN IA GENERATIVA EN LA CIENCIA DE DATOS

3.1. Riesgos potenciales y éticos específicos en IAG

3.2. Riesgos en la gestión del dato en IAG. La importancia de la privacidad y protección de datos

3.2.1 Riesgos e incompatibilidad con la normativa europea. Situación OpenAI

## CAPÍTULO 6.- LA CULTURA DE PRIVACIDAD

### 1. APROXIMACIONES CONCEPTUALES A LA PRIVACIDAD

### 2. CONSTRUYENDO LA CULTURA DE PRIVACIDAD

2.1. La implicación, liderazgo de la dirección y los altos mandos en la buena gobernanza de datos

2.2. La formación y los canales de comunicación

2.3. La importancia de la definición de los roles: La responsabilidad

2.4. La transparencia y agilidad en la cultura de privacidad

2.5. La interacción del departamento legal con el departamento IT

2.6. La cultura extensiva a clientes y proveedores

2.7. La resistencia al cambio y la motivación

### 3. LA IMPORTANCIA DE LAS AUDITORÍAS ALGORÍTMICAS Y LA CULTURA DE PRIVACIDAD

### 4. LAS CERTIFICACIONES Y LA CULTURA DE PRIVACIDAD Y SEGURIDAD

4.1. La norma ISO/IEC 27001

4.2. La norma ISO/IEC 42001

4.3. El certificado de Esquema Nacional de Seguridad

4.4. Otras ISO.