Instituto Tecnológico de Estudios Superiores de Monterrey,

Campus Querétaro

TC3007C.501

Inteligencia Artificial avanzada para la ciencia de datos

Actividad

Investigación de lineamientos de seguridad de datos

para proyectos de Inteligencia Artificial

Profesor

Dr. Benjamín Valdés Aguirre

Ma. Eduardo Daniel Juárez Pineda

Dr. Ismael Solis Moreno

Dr. José Antonio Cantoral

Dr. Carlos Alberto Dorantes

Presenta

Carlos Rodrigo Salguero Alcántara A00833341

Querétaro, Querétaro

Lunes 07 de octubre de 2024 a Sábado 02 de noviembre de 2024

Introducción **3**
Propósito 3
Alcance del Análisis 3
Análisis de Regulaciones **3**
Cumplimiento LFPDPPP (México) 3
Aspectos aplicables al proyecto 3
Artículos relevantes 4
Artículo 8 4
Artículo 19 4
Artículo 25 4
Consideraciones GDPR (Unión Europea) **4**
Aspectos aplicables 4
Base legal para el procesamiento de datos (Art. 6 - 11) 4
Transparencia y Comunicación (Art. 12 - 14) 5
Protección de datos por diseño (Art. 25, 5) 5
Seguridad interna (Art. 32 - 34) 5
Responsabilidad y supervisión (Art. 37 - 39) 5
Políticas específicas para Inteligencia Artificial (AI) **6**
Regulación Europea (AI Act) (Art. 5 - 7, 10, 14, 52) 6
Marco NIST para Gestión de Riesgos de Inteligencia Artificial 6
Acuerdo de Políticas de Datos, Ética y Seguridad (Proyecto) **6**
Políticas de Datos, Ética y Seguridad 6
Responsabilidad y cumplimiento 8
Incumplimiento de la Norma 9
Referencias **11**

Introducción

Este documento describe las políticas integrales de protección de datos para el proyecto de inteligencia artificial, asegurando el cumplimiento tanto con la regulación mexicana (LFPDPPP) como con la europea (GDPR). Las políticas aquí descritas están diseñadas para proteger los datos personales mientras se permite el desarrollo y despliegue efectivo de sistemas de IA para el análisis de imágenes de ganado.

Propósito

- Identificar las regulaciones aplicadas al proyecto de Inteligencia Artificial
- Analizar los requerimientos específicos de cada normativa
- Determinar las medidas necesarias para garantizar el cumplimiento legal
- Establecer un marco de referencia para la implementación de protecciones de datos

Alcance del Análisis

Este análisis se aplica a

- Captura y procesamiento de imágenes de ganado vacuno
- Manejo de datos personales incidentales
- Procesos de almacenamiento y gestión de datos

Análisis de Regulaciones

Cumplimiento LFPDPPP (México)

Aspectos aplicables al proyecto

- Definición y clasificación de datos capturados
- Requerimientos de consentimiento para datos personales
- Políticas de retención y eliminación de datos
- Protocolos para datos personales incidentales

Artículos relevantes

Artículo 8

El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.

Artículo 19

Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y fìsicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Artículo 25

El titular tendrá en todo momento el derecho a cancelar sus datos personales. La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia.

Consideraciones GDPR (Unión Europea)

Aspectos aplicables

Base legal para el procesamiento de datos (Art. 6 - 11)

El GDPR establece que todo procesamiento de datos debe tener una justificación legal específica bajo una de las seis condiciones establecidas en el Artículo 6. Para nuestro proyecto, es fundamental documentar claramente la base legal elegida para el procesamiento de datos. Si se elige el consentimiento como base legal, debemos implementar mecanismos que permitan a los usuarios revocar su consentimiento en cualquier momento. En caso de basarnos en intereses

legítimos, es necesario realizar y documentar una evaluación de impacto en la privacidad. Adicionalmente, debemos considerar las disposiciones especiales que aplican a datos sensibles, según lo establecido en los Artículos 7-11 del reglamento.

Transparencia y Comunicación (Art. 12 - 14)

La transparencia en el manejo de datos es esencial bajo el GDPR. Se requiere desarrollar una política de privacidad clara que explique detalladamente el propósito de la recolección de datos, los métodos de procesamiento empleados, quiénes tienen acceso a los datos y las medidas de seguridad implementadas. Esta información debe presentarse de manera concisa y transparente, utilizando un lenguaje sencillo que sea comprensible para cualquier usuario. La política debe estar fácilmente accesible y debe proporcionarse en el momento de la recolección de los datos.

Protección de datos por diseño (Art. 25, 5)

El principio de protección de datos por diseño requiere que implementemos medidas de protección desde las etapas iniciales del proyecto. Esto incluye tanto medidas técnicas, como el cifrado y sistemas de seguridad, como medidas organizativas que limiten la recolección de datos al mínimo necesario. Todo procesamiento de datos debe cumplir con los principios establecidos en el Artículo 5 del GDPR. Es fundamental establecer políticas claras de retención y eliminación de datos, asegurando que no se almacenen por más tiempo del necesario para cumplir con los propósitos establecidos.

Seguridad interna (Art. 32 - 34)

La seguridad operativa es tan importante como la seguridad técnica. Es necesario establecer una política de seguridad integral que incluya protocolos para el manejo seguro del correo electrónico, gestión de contraseñas robustas, implementación de autenticación de dos factores, cifrado de dispositivos y uso apropiado de VPNs. Todo el personal que tenga acceso a datos personales debe recibir capacitación específica sobre estos protocolos, y los empleados no técnicos deben ser instruidos en los requerimientos básicos del GDPR que afectan a sus funciones.

Responsabilidad y supervisión (Art. 37 - 39)

El cumplimiento del GDPR requiere la designación de un responsable específico dentro de la organización. Esta persona debe estar facultada para evaluar las políticas de protección de

datos, supervisar su implementación y asegurar el cumplimiento continuo de la normativa. El responsable debe tener la autoridad necesaria para implementar cambios y mejoras en los procesos de protección de datos cuando sea necesario.

Políticas específicas para Inteligencia Artificial (AI)

Regulación Europea (AI Act) (Art. 5 - 7, 10, 14, 52)

El AI Act establece un marco comprensivo para la regulación de sistemas de Inteligencia Artificial. Para el proyecto, es fundamental entender que se clasifica como un sistema de "riesgo limitado", lo que implica obligaciones específicas de transparencia y documentación. Se requiere informar a los usuarios sobre la interacción con un sistema de Inteligencia Artificial, documentar las capacidad y limitaciones del sistema, y establecer mecanismos de supervisión humana. La documentación técnica debe incluir metodologías de entrenamiento, conjuntos de datos utilizados y métricas de rendimiento.

Marco NIST para Gestión de Riesgos de Inteligencia Artificial

El Instituto Nacional de Estándares y Tecnología (NIST) proporciona un marco integral para la gestión de riesgos en sistemas de IA. Se requiere realizar evaluaciones periódicas de riesgo, gestionar adecuadamente el ciclo de vida del sistema y aplicar las mejores prácticas técnicas disponibles. Este marco es especialmente relevante para garantizar la robustez y fiabilidad del sistema.

Acuerdo de Políticas de Datos, Ética y Seguridad (Proyecto)

Este documento establece las políticas de datos, ética y seguridad para el manejo del proyecto, el cual es esencial la firma de todos los involucrados como compromiso con el cumplimiento de las normativas.

Políticas de Datos, Ética y Seguridad

1. **Retención de datos limitada y eliminación segura**
   Las imágenes recolectadas serán almacenadas únicamente durante el tiempo

estrictamente necesario para cumplir con los objetivos del proyecto. Una vez cumplido el propósito, se procederá a su eliminación segura mediante métodos aprobados (como borrado criptográfico) o se anonimizarán para proteger los datos personales y garantizar su uso ético en análisis futuros.

2. **Control de acceso restringido**

   Solo tendrán acceso a los datos las personas autorizadas que hayan firmado los acuerdos de confidencialidad correspondientes. Esto incluye el uso de credenciales únicas, restricciones de acceso físico a los servidores, y la implementación de sistemas de monitoreo para detectar accesos no autorizados.

3. **Autenticación robusta y contraseñas seguras**

   Todo el equipo deberá usar autenticación de dos factores para acceder a los datos y sistemas relacionados. Las contraseñas deberán cambiarse periódicamente para una mayor seguridad.

4. **Capacitación continua en seguridad de datos**

   Todo el personal deberá participar en capacitaciones regulares sobre temas de privacidad y seguridad, tales como la gestión de incidentes, protección frente a phishing, y mejores prácticas para el manejo de datos sensibles.

5. **Verificación de cumplimiento normativo**

   Se deberán realizar auditorías periódicas para asegurar que las prácticas del proyecto cumplen con las normativas LFPDPPP (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) y GDPR (Reglamento General de Protección de Datos). Esto incluye realizar revisiones de los contratos con terceros y las medidas de protección implementadas.

6. **Gestión ética de datos personales**

   Todos los datos recopilados deberán ser tratados de acuerdo con principios éticos. En caso de que las imágenes capturen a personas de forma incidental, su identidad deberá ser protegida mediante técnicas de anonimización o difuminado. Se prohíbe el uso de los datos para cualquier fin que no esté explícitamente aprobado en el proyecto.

7. **Prohibición de compartir datos sin autorización**

   Está estrictamente prohibido compartir datos o imágenes fuera del equipo autorizado del proyecto sin previa autorización de los docentes y del socio formador.. Esto incluye tanto datos crudos como procesados.

8. **Registro de uso y manejo de datos**

   Se deberá mantener un registro detallado de todos los accesos, descargas y usos de

los datos. Este registro incluirá la fecha, hora, propósito, y la identificación de la persona que accedió a los datos.

9. **Protección contra incidentes de seguridad**
   Todo el equipo está obligado a reportar inmediatamente cualquier incidente de seguridad, como accesos no autorizados, pérdida de datos, o posibles vulnerabilidades. Se implementarán medidas para mitigar riesgos futuros, como parches de seguridad y revisiones de los protocolos.
10. **Acuerdos de confidencialidad con terceros**
    Los proveedores o colaboradores externos deberán firmar un DPA (Acuerdo de Procesamiento de Datos) que estipule las medidas de seguridad requeridas y las consecuencias legales por incumplimiento.
11. **Revisión continua y mejora de políticas**
    Las políticas de seguridad serán revisadas y actualizadas regularmente para adaptarse a cambios tecnológicos, normativos, o de contexto en el proyecto. Se espera la participación activa del equipo para proponer mejoras.
12. **Transparencia y comunicación clara**
    Toda la información relacionada con el tratamiento de datos deberá ser comunicada de manera clara y accesible a todas las partes involucradas. Esto incluye las finalidades del tratamiento, las medidas de seguridad implementadas, y los derechos de los titulares de los datos.

Responsabilidad y cumplimiento

13. **Acuerdo de cumplimiento y NDA**

    Todo miembro del equipo y los representantes del socio empresarial deberán firmar un acuerdo en el que se comprometan a cumplir con estas políticas de manejo de datos. Este acuerdo incluirá un acuerdo de confidencialidad (NDA) que especificará las obligaciones de cada parte y la prohibición de divulgar datos o imágenes fuera del proyecto.

14. **Compromiso con el cumplimiento**

A través de la firma del acuerdo, todos los involucrados en el proyecto reafirman su compromiso de tratar los datos con la máxima responsabilidad, en alineación con las normativas aplicables y los principios éticos detallados en estas políticas.

Incumplimiento de la Norma

En caso de que alguna de las políticas descritas en este documento no sea cumplida por los involucrados, se procederá conforme a los siguientes puntos:

1. **Responsabilidad académica**

   Se evaluarán las implicaciones académicas del incumplimiento, y se tomarán las acciones necesarias conforme a las normativas vigentes. Esto incluye la notificación a las autoridades correspondientes y, en caso de ser necesario, la aplicación de sanción con el respectivo comité educativo donde se reportará como FIA (Falta de Integridad Académica) al estudiante que no cumpla con las normas establecidas.

2. **Acciones correctivas inmediatas**

   Se implementarán medidas correctivas para mitigar los efectos del incumplimiento. Esto incluye, pero no se limita a:

   - La suspensión temporal o permanente del acceso a los datos.
   - La rectificación inmediata de las vulneraciones a la seguridad o privacidad.
   - La reparación de daños ocasionados, si aplica.

3. **Revisión de procedimientos**

   El equipo de trabajo llevará a cabo una revisión exhaustiva de los procedimientos para identificar posibles fallos en la implementación de las políticas y proponer mejoras que prevengan futuros incumplimientos.

4. **Compromiso renovado**

   El involucrado deberá firmar un compromiso adicional que garantice la alineación de su conducta con las políticas descritas. En casos graves, se evaluará la continuidad de su participación en el proyecto.

5. **Notificación a partes interesadas**

Se informará a los responsables del proyecto y, de ser necesario, a los socios o terceros afectados sobre el incumplimiento, detallando las acciones tomadas para solventarlo.

Nosotros, como equipo de desarrollo, nos comprometemos a cumplir con las políticas descritas:

- **Nombre y firma: _____ Fecha: _____**
- **Nombre y firma: _____ Fecha: _____**
- **Nombre y firma: _____ Fecha: _____**
- **Nombre y firma: _____ Fecha: _____**
- **Nombre y firma: _____ Fecha: _____**

Yo, como socio formador del proyecto, confirmo estar de acuerdo con las políticas descritas:

- **Nombre y firma: _____ Fecha: _____**

Documento firmado por las partes interesadas: Políticas Privacidad y Seguridad de Datos.pdf

Referencias

Congreso Mexicano. (5 de julio de 2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Parlamento Europeo y Consejo. (27 de abril de 2016). Reglamento (UE) 2016/679 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. Diario Oficial de la Unión Europea, L119, 1-88. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2024). Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. INAI. http://inicio.inai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

Parlamento Europeo y Consejo. (2021). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas sobre la Inteligencia Artificial (Ley de IA). COM/2021/206 final. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021PC0206

National Institute of Standards and Technology. (2024). Artificial Intelligence Risk Management Framework (AI RMF 1.0). https://www.nist.gov/itl/ai-risk-management-framework

National Institute of Standards and Technology. (2023). AI Risk Management Framework: A Voluntary Framework. NIST Special Publication 1270. https://doi.org/10.6028/NIST.SP.1270