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

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.

Políticas seleccionadas para el proyecto grupal

Introducción

Este documento establece las políticas y lineamientos para el manejo ético y seguro de datos en el proyecto de monitoreo de ganado bovino mediante visión artificial en las instalaciones del CAETEC. Su propósito es garantizar la protección de datos personales, cumplir con las regulaciones vigentes y establecer prácticas seguras para todos los participantes del proyecto.

Propósito

- Definir los procedimientos para la recolección y manejo de datos visuales.
- Establecer protocolos de seguridad y privacidad.
- Asegurar el cumplimiento de normativas nacionales e internacionales.
- Proteger los derechos de privacidad de los individuos involucrados.
- Establecer responsabilidades y consecuencias del incumplimiento.

Glosario de términos

- **CAETEC**: Centro de Experimentación Agropecuaria del Tecnológico de Monterrey
- **LFPDPPP**: Ley Federal de Protección de Datos Personales en Posesión de los Particulares
- **GDPR**: Reglamento General de Protección de Datos (General Data Protection Regulation)
- **DPA**: Acuerdo de Procesamiento de Datos (Data Processing Agreement)
- **NDA**: Acuerdo de Confidencialidad (Non-Disclosure Agreement)

Anonimización de los datos

Es el proceso de eliminar o alterar identificaciones personales de conjuntos de datos para que no se pueda identificar a las personas. Su objetivo es proteger la privacidad, particularmente cuando se trata de información sensible. Los métodos de anonimización varían y pueden incluir técnicas como enmascaramiento de datos, seudonimización y generalización.

El conjunto de datos consiste principalmente en imágenes tomadas desde una perspectiva cenital (vista superior), capturadas desde una viga ubicada en el corral. La mayoría de estas fotografías muestran exclusivamente a las vacas en línea de espera para el ordeño, sin presencia humana ni información sensible. Si bien en algunas imágenes aparecen colaboradores del CAETEC realizando sus labores, la naturaleza de la toma área y el uso de sombreros por parte del personal hace que sus identidades no sean reconocibles, preservando su privacidad.

Políticas de datos, ética y seguridad

Alcance y tipos de datos

Tipos de datos capturados

- El proyecto implica la captura de datos visuales primarios, incluyendo imágenes cenitales en instalaciones de ordeño; sin embargo, imágenes con la presencia de personas pueden aparecer incidentalmente. Estas imágenes tienen perspectiva superior desde la estructura del corral.

Propósito de la recolección de datos

- El artículo 15 de LFPDPPP establece que el responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines. La recolección de datos está orientada a optimizar el monitoreo y el seguimiento del ganado y a mejorar la eficiencia operativa en la gestión de animales. Las imágenes de personas sólo se recopilan incidentalmente y no son el foco del procesamiento de datos.

Protocolos de privacidad y seguridad

Políticas de retención de imágenes

- Las imágenes serán conservadas únicamente durante el período mínimo necesario para cumplir con los objetivos del proyecto, y luego se eliminarán de forma segura o se anonimizarán según los requisitos de protección de datos.

Seguridad de datos y salvaguardias administrativas

El artículo 19 de LFPDPPP requiere que todo responsable de datos implemente medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción y uso no autorizado. Esto lo garantizamos con:

- Control de acceso restringido
- Almacenamiento seguro
- Auditorías periódicas
- Prevención de pérdida, alteración o uso indebido

Políticas de privacidad de imágenes

Las imágenes recolectadas estarán protegidas de acceso no autorizado y no se compartirán fuera del equipo del proyecto.

Derechos y cumplimiento normativo

Derecho de titulares de datos

El artículo 25 de LFPDPPP establece el derecho de los titulares a cancelar sus datos personales cuando hayan dejado de ser necesarios para la finalidad que fueron recabados.

- Derecho de cancelación de datos personales
- Procedimientos claros establecidos en aviso de privacidad

Cumplimiento del GDPR

- Justificación legal para el tratamiento de datos (artículo 6) establece las bases legales para el procesamiento de datos personales, incluyendo consentimiento, obligación legal, intereses legítimos, entre otros.
- Transparencia en el procesamiento de datos (artículo 12) requiere que toda información relacionada con el tratamiento de datos personales sea concisa, transparente, inteligible y de fácil acceso.

Protección de datos por diseño

Política de seguridad interna

- Autenticación de dos factores
- Gestión segura de contraseñas
- Prácticas seguras en comunicaciones
- Capacitación continua en seguridad de datos

Acuerdo de procesamiento de datos con terceros

- DPA con proveedores que cumplan estándares de seguridad
- Verificación de cumplimiento normativo.

Responsabilidad y cumplimiento

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.

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

- Responsabilidad académica y legal
- Acciones correctivas inmediatas
- Revisión de procedimientos

Proceso para trabajar con los datos

Propósito

El propósito de este proceso es establecer las directrices y procedimientos para el manejo de seguridad y ético del conjunto de datos del proyecto, especificando:

- Protocolos de almacenamiento y acceso de datos
- Restricciones de red
- Niveles de autorización y acceso
- Requisitos documentales y acuerdos necesarios
- Normativas de cumplimiento obligatorio

Alcance

Estas políticas aplican a:

- Conjunto de datos del ganado
- Datos derivados del procesamiento

- Información sensible incidental
- Documentación relacionada al proyecto

Involucrados

- Personal técnico del CAETEC
- Asesores académicos
- Equipo de desarrollo

Proceso

Entradas	**Salidas**
Presentación introductoria del proyecto	Registros de acceso a datos
Conjunto de datos de imágenes	Acuerdos firmados de confidencialidad
Documentación técnica relacionada	Documentación de cumplimiento
Requisitos legales y normativos	Reportes de auditoría

Pasos

Fase	Actividad	Responsable
Solicitud inicial	Presentar solicitud para el acceso de datos	Equipo de desarrollo
Acceso a datos	Verificar que el acceso otorgado sigue vigente	Equipo de desarrollo
	Confirmar que se han firmado todos los acuerdos necesarios (NDA)	
	Revisar las políticas de uso permitido	
Recolección	Acceder a los datos siguiendo los protocolos establecidos	Equipo de desarrollo
	Documentar fecha y hora de	

	obtención	
	Verificar que el uso previsto cumple con las normativas y permisos otorgados	
	Registrar cualquier anomalía encontrada	
Registro de uso	Documentar en el archivo “Gestión y registro de datos”: fecha y hora de acceso y propósito específico del uso	Equipo de desarrollo
	Cantidad de datos utilizados	
	Observaciones relevantes	
Manejo de datos	Utilizar los datos sólo para los fines autorizados	Equipo de desarrollo
	Mantener los datos en las ubicaciones aprobadas	
	No compartir accesos o datos con personas no autorizadas	
	Reportar cualquier incidente de seguridad	
Seguimiento	Mantener registro actualizado de uso	Diego Perdomo
	Verificar periódicamente que se siguen cumpliendo los términos de uso	
	Solicitar renovación de permisos cuando sea necesario	

Gestión y registro de los datos

El siguiente documento contiene el registro del manejo de los datos conforme al proceso establecido.

Gestion y Registro de Datos

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