Politicas de Datos

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 imagenes 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

Investigación Individual

1.0 Introducción

Las politicas de datos son reglas que regulan cómo se recopila, almacena, usa, protege y comparte la información dentro de una organización o proyecto. Estas ploiticas aseguran que los datos se manejen de forma etica, segura y conforme a las leyes y regulaciones vigentes, como el Reglamento General de Proteccion de Datos (GDPR).

Al trabajar en un proyecto de software como este en el cual utilizamos los datos del cliente las politicas que vayamos a definir son importantes.

- Protección del cliente: Las politicas de datos ayudan a garantizar que la información del cliente esté protegida.
- Cumplimiento legal: Existen regulaciones que establecen cómo deben manejarse los datos. Cumplir con las politicas de datos permite que la empresa esté alineada con estas regulaciones y evita sanciones legales.-
- Seguridad de la información: Las politicas de datos establecen controles de acceso, prácticas de encriptacióon y procedimientos de respaldo para proteger los datos contra accesos no autorizados.
- Gestión etica de los datos: Las politicas de datos aseguran que la información se use de forma etica.

2.0 Investigación

2.1 LFPDPPP

En México, el manejo de datos personales, incluyendo datos sensibles y cualquier información que pueda vincularse a una persona está regulado por la Ley Federnal de Protección de Datos Personales en Posesión de los Particulares. Esta ley y su reglamento establecen los lineamientos para proteger la información de personas físicas, regulando cómo las empresas y organizaciones deben tratar los datos personales y estableciendo medidas para su protección y correcto manejo.

Aunque las imágenes de vacas podrían no considerarse datos personales directos, si las imágenes contienen información o detalles que indirectamente podrían vincularse a la empresa o sus activos, sería prudente obtener consentimiento explícito para su uso. La LFPDPPP requiere que el titular de los datos (en este caso, la empresa propietaria de las vacas) otorgue autorización para recolectar, usar y procesar dicha información.

Capítulo 2:

- Artículo 6.- Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.
- Artículo 9.- Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca. No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.
- Artículo 15.- El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.

Capítulo 4:

- Artículo 28.- El titular o su representante legal podrán solicitar al responsable en cualquier momento el acceso, rectificación, cancelación u oposición, respecto de los datos personales que le conciernen.

2.2 GDPR

El Reglamento General de Protección de Datos (GDPR) de la Unión Europea contiene varios artículos (o "recitales") relevantes para los temas de confidencialidad, seguridad y manejo adecuado de los datos en el contexto empresarial.

Recital 52: Exceptions to the Prohibition on Processing Special Categories of Personal Data

- Destaca la importancia de las salvaguardas para proteger los derechos y libertades de los titulares de los datos, asegurando un balance entre los intereses del controlador de los datos y la protección de los datos.

Recital 85: Notification Obligation of Breaches to the Supervisory Authority

- Se establece que si ocurre una violación de datos personales, debe notificarse a la autoridad de protección de datos en un plazo de 72 horas.

2.3 ISO 27001

Estos estándares ayudan a las empresas a establecer un sistema de gestión de la seguridad para proteger los datos contra ataques, accesos no autorizados y otras amenazas cibernéticas.

La norma ISO 27001 se aplica a cualquier tipo de organización, incluyendo pequeñas y medianas empresas, grandes corporaciones, instituciones gubernamentales y sin fines de lucro. También se puede aplicar en cualquier sector, incluyendo tecnología de la información, finanzas, salud y servicios públicos.

2.4 Ley Federal de Protección a la Propiedad Industrial (LFPPI)

El artículo 165 señala que se considerará como uso indebido de información confidencial cuando una persona, sin el consentimiento del titular, explote o divulgue información considerada como secreto industrial.

- Artículo 165.- La persona que ejerza el control legal del secreto industrial podrá transmitirlo o autorizar su uso a un tercero. El usuario autorizado tendrá la obligación de no divulgar el secreto industrial por ningún medio. En los convenios por los que se transmitan conocimientos técnicos, asistencia técnica, provisión de ingeniería básica o de detalle, se podrán establecer cláusulas de confidencialidad para proteger los secretos industriales que incluyan, las cuales deberán precisar los aspectos que comprenden como confidenciales.

El artículo 170 permite la divulgación de información protegida bajo ciertas condiciones, como acuerdos expresos y con medidas adecuadas de confidencialidad.

- Artículo 170.- Cualquier persona, física o moral, podrá hacer uso de marcas en la industria, en el comercio o en los servicios que presten. Sin embargo, el derecho a su uso exclusivo se obtiene mediante su registro en el Instituto.

Referencias:

- De Diputados, Cámara, et al. *LEY FEDERAL de PROTECCIÓN a LA PROPIEDAD INDUSTRIAL LEY FEDERAL de PROTECCIÓN a LA PROPIEDAD INDUSTRIAL TEXTO VIGENTE Nueva Ley Publicada En El Diario Oficial de La Federación El 1 de Julio de 2020*, https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.
- GDPR. "General Data Protection Regulation (GDPR)." *General Data Protection Regulation (GDPR)*, 2016, gdpr-info.eu/https://gdpr-info.eu/recitals/
- "La Protección de Datos En La UE." *Commission.europa.eu*, commission.europa.eu/law/law-topic/data-protection/data-protection-eu_es.
- *Normativa Y Legislación En PDP – Marco Internacional de Competencias de Protección de Datos Personales Para Estudiantes*. micrositios.inai.org.mx/marcocompetencias/?page_id=370.
- Social, Instituto Nacional de Desarrollo. "Ley Federal de Protección de Datos Personales En Posesión de Los Particulares." *Gob.mx*, www.gob.mx/indesol/documentos/ley-federal-de-proteccion-de-datos-personales-en-posesion-de-los-particulares.
- Solutions, GlobalSuite. "¿Qué Es La Norma ISO 27001 Y Para Qué Sirve?" *GlobalSuite Solutions*, 20 Mar. 2023, www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/.