Análisis de Seguridad, Cumplimiento y Trazabilidad de Acceso para el Reto en Equipo

Gabriela Chimali Nava Ramírez | A01710530

09/11/2025

Índice

1. Análisis del Ecosistema de Datos y Marco Regulatorio
    1.1 El Ecosistema de Datos SINIIGA: Activos y Clasificación
    1.2 Análisis del Marco Legal Mexicano
2. Evaluación de Riesgos de Privacidad y Reidentificación para SINIIGA
3. Estrategia de Desasociación de Datos y Control de Riesgos (Cumplimiento SEG0403B-1)
    3.1 Anonimización
4. Propuesta de Gestión de Acceso y Gobernanza de Datos
    4.1 Verificación de Anonimización y Diagnóstico del Dataset
    4.2 Estándares de la Industria y Normativa Aplicable
    4.3 Proceso de trabajo seguro
5. Política de acceso en Equipo
6. Bitácora de cambios en Equipo
7. Referencias

1. Análisis del Ecosistema de Datos y Marco Regulatorio

1.1 El Ecosistema de Datos SINIIGA: Activos y Clasificación

El Sistema Nacional de Identificación Individual de Ganado (SINIIGA) de México fomenta la trazabilidad y sanidad agropecuaria del país. Mediante la asignación de una numeración única, permanente e irrepetible a cada animal (bovinos y colmenas) durante toda su vida[1] Esta numeración se materializa en un dispositivo de identificación (arete)[2].

Estos datos se consolidan en un "Banco Central de Información" (BCI) y se vinculan en la "Cédula de Identificación" es el documento de campo que conecta los datos del dispositivo de identificación del animal con la "Unidad de Producción Pecuaria (UPP) de origen y al primer propietario"[1] Esta "Clave UPP" se asigna a los productores al inscribirse en el Padrón Ganadero Nacional (PGN).

Para diseñar una arquitectura de seguridad y privacidad para el proyecto, es necesario clasificar estos activos de datos según los estándares de la industria:

- **Microdatos (Identificadores Directos):** Permiten la identificación directa de un individuo. En el contexto del SINIIGA, esto incluye toda la información asociada al propietario, como el Nombre completo del productor, su Registro Federal de Contribuyentes (RFC) y su domicilio fiscal o social.
- **Quasi-Identificadores (Datos de Identificación Indirecta):** Aunque no identifican directamente a una persona, pueden combinarse con otras fuentes para lograr la reidentificación. En este sistema, la Clave UPP es el de más alto riesgo. Aunque es alfanumérica, conecta la identidad del productor (en el PGN) con sus actividades (en el BCI). Otros quasi-identificadores

podrían ser coordenadas geográficas de la UPP, el municipio, el tipo de ganado y el tamaño del hato.

- **Datos Sensibles:** Información que revela aspectos confidenciales del individuo. En este caso, incluirían datos financieros (valor del hato), información sanitaria (enfermedades reportadas) o afiliaciones gremiales del productor.

1.2 Análisis del Marco Legal Mexicano

La Norma Oficial Mexicana NOM-001-SAG/GAN-2015 establece que la operación y resguardo del BCI es responsabilidad de la Secretaría (actualmente SADER)[3].

La NOM-001-SAG/GAN-2015 determina que los datos de los productores "estarán protegidos de acuerdo a lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental" (LFTAIPG). La LFTAIPG es una ley centrada en la transparencia y el acceso a la información pública, no como marco para la privacidad y protección de datos personales.

Esta ley exige el cumplimiento de principios estrictos, que incluyen:

- **Principio de Licitud:** Tratar los datos conforme a las atribuciones legales.
- **Principio de Finalidad:** Usar los datos sólo para los fines concretos y lícitos para los que fueron recabados.
- **Principio de Lealtad:** Prohíbe obtener y tratar datos "a través de medios engañosos o fraudulentos"..

Tabla 1: Clasificación de Activos de Datos SINIIGA y Régimen Legal Aplicable

Activo de Dato	**Clasificación de Privacidad**	**Riesgo Primario de Reidentificación**	**Ley Aplicable**
Número de Arete SINIIGA	Identificador (del animal)	Vinculabilidad (con la UPP)	NOM-001-SAG/GAN -2015
Tamaño del Hato, Reportes Sanitarios	Dato Sensible (Financiero/Salud)	Inferencia	LGPDPSO - Deber de Confidencialidad

2. Evaluación de Riesgos de Privacidad y Reidentificación para SINIIGA

El proceso de anonimización no es absoluto; se gestiona como un riesgo residual. Para gestionar este riesgo, se definen los riesgos principales de reidentificación:

1. **Singularización (Singling out):** Mide la posibilidad de extraer de un conjunto de datos algunos registros (o todos los registros) que identifican a una persona.
2. **Vinculabilidad (Linkability):** Mide la capacidad de vincular como mínimo dos registros en el mismo conjunto de datos o en dos conjuntos de datos distintos. Un atacante podría mezclar datasets (data blending), uniendo la Clave UPP con registros públicos de propiedad para de-anonimizar la riqueza de los productores.
3. **Inferencia (Inference):** Mide la posibilidad de deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos. Por ejemplo,

deducir el estado sanitario o económico de una región completa

3. Estrategia de Desasociación de Datos y Control de Riesgos (Cumplimiento SEG0403B-1)

Para abordar los riesgos identificados debe diseñarse diseñar una estrategia de desasociación de datos.

3.1 Anonimización

Los datos anonimizados son datos que han pasado por un proceso (ej. generalización, aleatorización) que imposibilita identificar al propietario". Estos datos ya no se consideran datos personales y no están sujetos a la LGPDPSO.

4. Propuesta de Gestión de Acceso y Gobernanza de Datos

Entendido lo anterior, para garantizar la seguridad de la información durante el desarrollo del proyecto, se analizaron los *datasets* recibidos y se buscan establecer los controles necesarios según las mejores prácticas de la industria.

4.1 Verificación de Anonimización y Diagnóstico del Dataset

Se realizó una inspección de los activos de información proporcionados por el Socio Formador para determinar el nivel de riesgo y eficacia de la anonimización actual:

- **Archivos de Producción (.csv):** Contienen variables técnicas de ordeño ("Sangre", "Flujo máximo por pezón", “Producción (kg)” entre otras).
    - Se detectó que el campo "Usuario" se encuentra vacío y el identificador de las vacas es un número secuencial de control interno.
    - Estos datos se consideran pseudonimizados de bajo riesgo. Al usar un ID interno secuencial en lugar del arete SINIIGA oficial, no es posible para alguien externo vincular estos datos con una vaca específica o su propietario sin tener acceso a la "llave" o tabla maestra del rancho. No se requieren acciones adicionales sobre los CSV, siempre y cuando se mantengan separados de la tabla de identidades.

- **Repositorio de Imágenes en Microsoft Drive (3 carpetas):** Son fotografías tomadas en sitio (establos y áreas de manejo).
    - Riesgo de Reidentificación Alto: A diferencia de los CSV, las imágenes no están anonimizadas. Debido al volumen masivo de archivos, es imposible revisar una por una para censurar los aretes SINIIGA visibles. Además, los fondos de las imágenes revelan infraestructura y ubicación geográfica que podría facilitar la localización del rancho.
    - Debido a esto, todo el set de imágenes debe tratarse bajo la clasificación de "Confidencialidad Estricta". No se permite su publicación ni exposición en reportes públicos sin un pre-procesamiento de desenfoque (blurring) de rostros humanos y números de arete.

4.2 Estándares de la Industria y Normativa Aplicable

Para el manejo de datos en el sector agroalimentario digital, se consultaron las directrices de la norma **ISO/IEC 27001** (Seguridad de la Información)[5] y las recomendaciones del **INAI** para el manejo de datos personales en posesión de particulares.[6]

Los pasos comunes en la industria para garantizar la privacidad en este tipo de proyectos incluyen:

- **Principio de Mínimo Privilegio:** Nadie debe tener acceso a la totalidad de los datos si no es estrictamente necesario.
- **Cifrado en Reposo:** Los datos no deben almacenarse en discos duros sin cifrado (BitLocker/FileVault).
- **Trazabilidad de Accesos:** En la industria es obligatorio mantener *logs* (registros) de quién accede, modifica o descarga un archivo.

4.3 Proceso de trabajo seguro

Actualmente, los datos fueron descargados a ordenadores personales y compartidos mediante transferencia directa entre miembros. Para mitigar esto, se sugiere el siguiente protocolo.

La fuente oficial de datos será una carpeta compartida en Google Drive Institucional (protegido por autenticación de la organización). Quedando prohibido enviar archivos de datos “peer-to-peer” por correo, WhatsApp, Telegram o USB entre miembros. Todo intercambio y extracción debe ser por la fuente oficial establecida.

El acceso a datos confidenciales no debe realizarse a través de redes WiFi públicas no seguras a menos que se utilice una VPN. Se recomienda el uso de redes domésticas privadas o la red del campus (Tec de Monterrey).

Dado que el trabajo se realiza en equipos personales, se establece la política de "Limpieza al terminar" en la que los archivos descargados temporalmente para su procesamiento en local, como el entrenamiento de modelos, deben ser eliminados de la carpeta local y papelera al finalizar la sesión de trabajo.

Antes de recibir permisos de edición en el Drive, cada miembro debe haber leído y aceptado (firma digital) las políticas de acceso definidas en el equipo.

5. Política de acceso en Equipo

https://abalone-timbale-4a2.notion.site/Pol-tica-de-acceso-287a3ea0df618097b208f5f04539b31c

6. Bitácora de cambios en Equipo

https://docs.google.com/spreadsheets/d/1H4hMijn9OsxfHKDEhNZj7_t2ieoMNB2_zAa0QC1PRjc/edit?usp=sharing

7. Referencias

1. *SINIIGA. Sistema Nacional de Identificación Individual de Ganado*. (s.f.). http://www.siniiga.org.mx/index.html
2. VENTANILLA AUTORIZADA SINIIGA JALISCO. (s.f.). *IDENTIFICADORES (ARETES) SINIIGA*. https://siniigajalisco.jimdofree.com/identificaci%C3%B3n-individual/identificadores-aretes/
3. De Agricultura Y Desarrollo Rural, S. (s.f.). *NOM-001-SAG/GAN-2015, SINIDA (Arete amarillo)*. gob.mx.

https://www.gob.mx/agricultura/documentos/nom-001-sag-gan-2015-sinida-arete-amarillo

4. *LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS*. (s.f.). https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

5. IBM (s.f.). *What is ISO/IEC 27001? | IBM*. https://www.ibm.com/products/cloud/compliance/iso-27001

6. *LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES*. (s.f.). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf