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

Gabriela Chimali Nava Ramírez | A01710530

09/11/2025

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. Su función principal es asignar 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].

El sistema está diseñado para consolidar toda esta información en un "Banco Central de Información" (BCI). El vínculo entre estos datos se crea en el punto de origen: 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, se clasifican estos activos de datos según los estándares de la industria:

- **Microdatos (Identificadores Directos):** Son datos que 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):** Son datos que, 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 un código alfanumérico, 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:** Se refieren a 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.

Se identifica la Clave UPP como el activo más peligroso desde la perspectiva de la privacidad. Proteger el número de arete individual ya que la Clave UPP puede vincularse a la identidad del productor y, con esto, a sus datos sensibles.

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 un marco para la privacidad y protección de datos personales.

El operador del BCI (SADER) es una entidad gubernamental, llamado "sujeto obligado". Por lo tanto, el marco legal aplicable y de mayor jerarquía es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO)[4].

Esta ley impone un estándar de cumplimiento mucho más elevado. Exige a la SADER y a los operadores del BCI 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".
- **Deber de Confidencialidad:** (Art. 42 LGPDPSO) Obliga al responsable (SADER) a establecer controles para que todas las personas que intervengan en el tratamiento de los datos guarden confidencialidad, obligación que persiste indefinidamente.[16]

Por lo tanto, la arquitectura de seguridad no debe diseñarse para el estándar mínimo de la LFTAIPG, sino para el estándar máximo del "Deber de Confidencialidad" exigido por la LGPDPSO.

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

Activo de Dato	**Clasificación de Privacidad**	**Riesgo Primario de Reidentificación**	**Ley Aplicable**
Nombre del Productor, RFC, Domicilio	Microdato	Singularización	LGPDPSO - Deber de Confidencialidad
Clave UPP (Unidad de Prod. Pecuaria)	Quasi-Identificador	Vinculabilidad	LGPDPSO - Deber de Confidencialidad
Coordenadas Geográficas (Predio)	Quasi-Identificador	Vinculabilidad, Inferencia	LGPDPSO - Deber de Confidencialidad
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... ya sea en el mismo conjunto de datos o en dos conjuntos de datos distintos.
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.

El riesgo de reidentificación suele aumentar con el paso del tiempo, debido a la posible aparición de nuevos datos.

2.1 Aplicación de Riesgos al Contexto SINIIGA

Al aplicar estos vectores al ecosistema SINIIGA, emergen amenazas claras:

- **Riesgo de Singularización:** Un atacante que ya conoce la identidad de un productor “N”, podría consultar un conjunto de datos SINIIGA supuestamente anónimo. Si “N” es el único productor de ganado en el municipio X, su registro puede ser singularizado, revelando cualquier otro dato sensible asociado a él.
- **Riesgo de Vinculabilidad**: La documentación de seguridad advierte sobre el riesgo de "mezclar dataset con otras fuentes". La Clave UPP es un identificador gubernamental, lo que hace altamente probable que exista en múltiples bases de datos públicas).
  Un atacante podría ejecutar un ataque de *data blending* (mezcla de datos) simple:
  1. Obtener legalmente un conjunto de datos de registros de propiedad de la tierra, que incluye la Clave UPP y el nombre del propietario.
  2. Obtener un conjunto de datos SINIIGA "anonimizado" (Dataset B), que ha eliminado los nombres pero aún contiene la Clave UPP y el tamaño del hato.
  3. Realizar una operación de JOIN (unión) en ambos datasets usando la Clave UPP como clave de vínculo.
     El resultado es una de-anonimización instantánea y completa de la riqueza de cada propietario de tierras en México.
- **Riesgo de Inferencia:** Este riesgo más que de privacidad individual y se convierte en un riesgo de inteligencia económica y seguridad nacional. Un atacante puede no estar interesado en un productor individual, sino en la salud agregada de regiones clave.
  Incluso en un conjunto de datos generalizado, si un atacante observa que en la "Región X", el 80% de los hatos reportan una enfermedad específica, pueden inferir con alta probabilidad la salud del hato de cualquier productor de esa región. Incluso patrones de enfermedad, sequía o liquidación de hatos antes de que los informes oficiales se publiquen. Permitiéndole manipular los mercados de futuros de carne, predecir la inestabilidad económica regional o crear escasez artificial.

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.

El cifrado por hash simple (ejemplo, SHA256) es una técnica de seudonimización débil. Es vulnerable a ataques de fuerza bruta o de diccionario, y si se usa el mismo hash para el mismo valor, ya que permite la vinculabilidad.

3.2 Estrategia Híbrida por Capas

La solución es una arquitectura de datos por capas, donde cada capa sirve a un propósito diferente y utiliza una técnica de privacidad adecuada:

Capa 1: Base de Datos de Producción (Seudonimizada para Uso Interno)

- **Técnica:** Seudonimización (Tokenización) Robusta.
- **Implementación:**
  1. Todos los Microdatos (RFC, Nombre, Domicilio) se remplazan por *tokens* (seudónimos).
  2. Para evitar los riesgos del hash simple, se usará un algoritmo de hash robusto como Blake2b).
  3. Se aplicará un *salt,* es decir, un valor aleatorio que se añade antes de aplicar el hash. Se aplicará un dominio, ej. domain=b'SINIIGA_BCI'. Esto asegura que el token generado para este sistema sea diferente al token para un individuo en cualquier otro sistema, mitigando el riesgo de vinculabilidad.

Capa 2: Vista Analítica Pública (Anonimizada para Transparencia)

- **Técnicas:** Generalización y aleatorización.
- **Implementación:**
  1. Se aplicará el K-Anonimato. Esta técnica de generalización garantiza que cada registro sea indistinguible de al menos $K-1$ otros registros. Para lograr esto, se generalizarán los quasi-identificadores:

1. Las Claves UPP se agruparán en categorías geográficas superiores (ejemplo, "Municipio" o "Región AGS").
2. Siguiendo el método las características del hato se discretizan en rangos.

  2. El K-Anonimato por sí solo es vulnerable a ataques de inferencia. Para mitigar esto, se aplicará la Adición de Ruido. Se añadirá ruido estadísticamente insignificante a la información sensible de hatos o reportes sanitarios. Esto mantiene los patrones estadísticos generales pero hace imposible que un atacante confíe en la inferencia.

3. Política de acceso en Equipo

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

4. 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