Política de acceso

Propósito

En este documento se establece la política de acceso a las imágenes y archivos CSV del proyecto del CATEC que debe seguir el equipo para proteger la integridad y la trazabilidad de la investigación.

Esto es esencial para mantener la validez de los datos y prevenir su pérdida o modificación accidental. Al mismo tiempo manteniendo información sensible siempre protegida y fuera del alcance de terceros que no estén involucrados en el proyecto.

Alcance

La protección de datos aplica a los datos obtenidos del CAETEC. Esto implica las imágenes de las vacas en los establos, así como los archivos de la producción de la leche generados por la máquina de ordeño. La información confidencial del CAETEC queda dentro del alcance. Entiéndase como confidencial un elemento de información proporcionado sobre el CAETEC del cual no se desee que sea de dominio público.

Cualquier otra información no estipulada anteriormente queda fuera de la política de manejo de datos.

Riesgos

Los riesgos que existen en este proyecto respecto al uso de la información del cliente son:

1. Riesgos legales
    a. Violación de acuerdos de confidencialidad
    b. Uso indebido de identificadores oficiales de animales (SINIIGA)
    c. Falta de trazabilidad o registros auditables
    d. Exportación o manejo de datos transfronterizos sin regulación
2. Riesgos técnicos

    a. Pérdida de información
    b. Acceso no autorizado
    c. Filtración de información
    d. Malware o ransomware
3. Riesgos éticos y de privacidad
    a. Uso no autorizado de imágenes
    b. Difusión o publicación sin consentimiento
    c. Falta de consentimiento informado
4. Riesgos operativos
    a. Interrupción del proyecto por incumplimiento de regulaciones
    b. Daño financiero directo por multas, sanciones o litigios
    c. Pérdida de propiedad intelectual
    d. Desconfianza del cliente
5. Riesgos reputacionales e institucionales
    a. Afectación a la marca o institución
    b. Reputación de los colaboradores

Regulaciones y estándares implicados

- En el aspecto ganadero:
    - NORMA OFICIAL MEXICANA NOM-001-SAG/GAN-2015, SISTEMA NACIONAL DE IDENTIFICACIÓN ANIMAL PARA BOVINOS Y COLMENAS
- En el manejo de los datos:
    - ISO/IEC 27001

Plan de Mitigación de Riesgos de Seguridad de la Información

Basado en ISO/IEC 27001:2022

1. Identificación y clasificación de los datos
   Mitigación esperada: reduce el riesgo de exposición por desconocimiento del nivel de confidencialidad.
   a. Inventariar todos los activos de información (A.5.9 – Inventario de activos de información).
      i. El inventario de los datos y su información relevante se encuentra en Reporte de Data Understanding
   b. Clasificar los datos según su sensibilidad: público, y confidencial (A.5.12 – Clasificación de la información).
      i. Únicamente los clasificamos en público y confidencial. Lo que se encuentra en el portal de Notion es de acceso público y el contenido confidencial en el drive.
2. Control de acceso y autenticación
   Mitigación esperada: evita accesos indebidos y abuso de privilegios internos.
   a. Implementar políticas de acceso mínimo necesario (A.5.15 – Control de acceso).
      i. Los repositorios están únicamente habilitados para profesores y miembros del equipo.
      ii. La carpeta de drive del proyecto está únicamente habilitados para profesores y miembros del equipo.
      iii. El acceso a las imágenes originales de Queue y Beds está únicamente permitido a los que hicieron la solicitud inicial (Chimali e Imanol)
   b. Autenticación multifactor (A.5.17 – Gestión de credenciales de autenticación).
      i. El acceso a las plataformas github y drive requiere de autenticación multifactor para poder acceder a la información.
   c. Revocación de acceso inmediato al miembro que sea dado de baja del equipo (A.6.3 – Ciclo de vida del acceso del usuario).
      i. Actualmente no se ha suscitado esta situación.
3. Protección física
   Mitigación esperada: minimiza la manipulación o robo físico de activos y

equipos.

   a. Restringir el acceso físico a las áreas donde se almacena o procesa información sensible (A.7.4 – Seguridad física).

      i. Dado que el proyecto se realiza en los dispositivos personales, no es posible limitar el acceso a estos, sin embargo, el espacio de trabajo dentro de las instalaciones del campus limita el acceso a personas que no pertenezcan a la comunidad.

4. Gestión de proveedores y terceros
   Mitigación esperada: evita filtraciones a través de terceros.

   a. Incluir cláusulas de confidencialidad y cumplimiento normativo en los contratos (A.5.19 – Seguridad de la información en relaciones con terceros).

      i. En este documento detallamos las cláusulas de confidencialidad y cumplimiento normativo con nuestro cliente: Memorándum de Políticas de Tratamiento y Acceso a Datos

   b. Supervisar el cumplimiento mediante auditorías o revisiones periódicas.

      i. La supervisión del cumplimiento será evaluada por los profesores en los momentos de retroalimentación.

5. Concientización y capacitación
   Mitigación esperada: reduce errores humanos y negligencia.

   a. Capacitar regularmente al personal en temas de protección de datos, phishing, uso responsable de sistemas y cumplimiento legal (A.6.3 – Concientización y formación).

      i. Cada uno de los miembros del equipo leyó conscientemente este documento, participó en su creación y estuvo de acuerdo con lo establecido.

   b. Establecer políticas disciplinarias ante incumplimientos.

      i. De no poder evidenciar la compresión o presentar incumplimientos de esta política se verán afectados en la obtención de las competencias de su malla de evaluación

6. Copias de seguridad y recuperación
   Mitigación esperada: protege la disponibilidad de la información frente a desastres o pérdidas.

a. Implementar un sistema de backups (A.8.13 – Copias de seguridad).
    i. Los repositorios que manejamos hace backups automáticamente.
    ii. El drive contiene las versiones de los datos a las cuales volver en caso de ser necesario.
    iii. Los datos del cliente se encuentran respaldados en un disco duro externo.
b. Almacenar copias en sitios geográficamente distintos.
    i. Los datos se encuentran en los servidores de las aplicaciones y también localmente en nuestros dispositivos y disco duro.

7. Respuesta ante incidentes
   Mitigación esperada: reduce el impacto de brechas y mejora la capacidad de reacción.
    a. Crear un procedimiento formal de gestión de incidentes (A.5.25 – Gestión de incidentes de seguridad de la información).
        i. Filtración de información confidencial:
            1. En caso de ser posible elimina la información filtrada de la plataforma lo antes posible.
            2. En caso de que personas ajenas al proyecto hayan visto o posean la información, comunica las implicaciones legales a las que podrían se acreedores en caso de que utilicen esa información.
            3. Comenta al equipo la filtración y por qué sucedió en el canal de comunicación del equipo.
            4. Comunica al cliente sobre la filtración.
            5. Actualiza este documento con la información necesaria para evitar repeticiones en el futuro.
            6. Si no existe aún, crea en este documento un log de filtraciones.

8. Documentación y cumplimiento legal
   Mitigación esperada: garantiza cumplimiento normativo y evita sanciones legales.
    a. Mantener políticas y procedimientos documentados (A.5.1 – Políticas de seguridad).

i. Este documento cumple con ese propósito.

b. NOM-001-SAG/GAN-2015.

i. La información de identificación oficial del ganado que se encuentra en su oreja, pudiera se legible en alguna imagen. Consecuentemente estos datos serán tratados como confidenciales.

Gestión de cambios

Actualmente, los datos del proyecto se almacenan en Google Drive. A continuación, se detallan las diferencias de registro, respaldo y eliminación de datos que se presentarían entre ambos.

	Google Drive
Registro de cambios	Se utiliza el historial de actividad de Google Drive para identificar quién modificó cada archivo y en qué momento. Además, se lleva una bitácora manual en una hoja de cálculo compartida, donde se registran las acciones relevantes sobre los archivos como las subidas, modificaciones de archivos, eliminaciones, restauraciones y cambios en permisos de acceso.
Eliminación de datos	Primeramente, se traslada el archivo a la papelera y posteriormente se elimina de forma definitiva después de un periodo determinado. Cada eliminación se documenta en la bitácora.

Responsabilidad de los usuarios

- Está prohibido compartir las credenciales de acceso de la gestión de identidad con cualquier persona, incluso con otros miembros del equipo.
- Está prohibido compartir los datos a terceros por medios que no sean la plataforma central de almacenamiento o los sistemas de acceso definidos.
- El usuario es responsable de eliminar de manera segura cualquier copia local temporal de los datos del proyecto una vez que su tarea haya finalizado.
- Toda acción realizada por el usuario en la plataforma (lectura, escritura, modificación o eliminación) se registra en la bitácora de cambios bajo su identidad única. El usuario es responsable de todas las acciones que se realicen bajo su cuenta.

Control de cambios

Versión	Descripción	Autor	Fecha
v1.0	Línea base	Ⓓ Diego Lira García	@13 de octubre de 2025
v1.1	Quitar la parte de AWS	Ⓓ Diego Lira García	@13 de octubre de 2025