Jorge Martínez López - a01704518@tec.mx
Adrián Matute Beltrán - a01703889@tec.mx
Andres Callealta - a01763701@tec.mx
José Pablo Martínez Valdivia - a01275676@tec.mx
Osvaldo Del Valle Mejía - a01275702@tec.mx

TÉRMINOS DE PRIVACIDAD Y AVISOS

Por este medio, el equipo de trabajo, conformado por Adrián Matute Beltrán, Andrés Callealta, José Pablo Martínez Valdivia, Osvaldo Del Valle Mejía y Jorge Martínez López, haremos hincapié en los siguientes lineamientos de privacidad y avisos, con el objetivo darles a conocer los procesos a la que será sometida la información compartida por el asesor del socio formador, Ivo Neftali Ayala García.

Primeramente, cabe mencionar que la información compartida por el socio formador (documentos, imágenes, tabla de información y código) será de índole académico,con el fin desarrollar prototipos y/o conocimiento para la elaboración del proyecto final de séptimo semestre de la concentración de Inteligencia Artificial Avanzada, que consiste en el desarrollo de un modelo inteligente para la detección de vacas lecheras. Cabe recalcar que el trabajo final se le compartirá al socio formador en la siguiente fecha 18/11/2024, a su vez los estudiantes que hayan participado en el proyecto tendrán la posibilidad de compartir el trabajo de forma pública, una vez de haber compartido lo correspondiente (proyecto completo y resultados) al socio formador.

Seguridad:

Para garantizar la seguridad de los datos y el acceso controlado en cada fase del proyecto, hemos implementado las siguientes medidas:

1. Acceso controlado a los datos del proyecto:
    a. Acceso a datos: Solo el equipo de trabajo asignado y los socios formadores tienen acceso a los datos (fotos del dataset) utilizados en el proyecto. Los datos están almacenados en Google Drive, protegido con permisos de usuario específicos, asegurando que solo personas autorizadas puedan visualizar o modificar la información.
    b. Control de usuarios: Los datos sensibles son todas aquellas fotos en donde salen trabajadores del CAETEC. Están protegidas y su acceso es monitorizado mediante logs de acceso para asegurar un uso adecuado.

2. Servidor y almacenamiento de datos:
    a. Servidor en Node.js: Configurado para trabajar en una Raspberry Pi, donde se ejecuta de manera local y asegura el procesamiento en tiempo real de los datos. Este servidor opera bajo protocolos de red seguros que protegen la comunicación con los dispositivos del sistema.
    b. Base de datos en línea con acceso controlado: La base de datos del proyecto se encuentra alojada en un servidor seguro en la nube. Para acceder a los datos, cada solicitud debe autenticarse mediante llaves de acceso únicas, garantizando que solo dispositivos y usuarios autorizados puedan interactuar con la base de datos. Las llaves de acceso están cifradas almacenadas de manera segura, de forma que el servidor local en la Raspberry pueda comunicarse sin comprometer la seguridad de los datos.

Tecnológico de Monterrey

Jorge Martínez López - a01704518@tec.mx
Adrián Matute Beltrán - a01703889@tec.mx
Andres Callealta - a01763701@tec.mx
José Pablo Martínez Valdivia - a01275676@tec.mx
Osvaldo Del Valle Mejía - a01275702@tec.mx

El proveedor de la base de datos se identifica como Turso, el cual se encuentra ubicado en Guadalajara, la base de datos a utilizar es de tipo SQLite.

Al usar una interfaz web, usaremos el protocolo HTTPS, el cual es útil para proteger las comunicaciones entre el servidor web y el navegador.

Firma