Privacidad y Seguridad de los Datos

Imanol Muñiz Ramirez A01701713

Sintetizamos las investigaciones individuales sobre la privacidad y seguridad de los datos en el siguiente documento de notion: Políticas de acceso y monitoreamos el uso de estos con el archivo: Bitácora de cambios

De mi análisis e investigación individual, concluí que los datos no contienen datos personales o que puedan dirigir a la identificación de una persona por lo que no es necesario anonimizar los datos. Dado que sólo son datos de animales (que no están protegidos por leyes como LFPDPPP o el RGPD) sólo debemos atender el manejo de estos en acuerdo con el propietario con el objetivo de evitar utilizarlos para propósitos ajenos a los intereses del cliente o que la información quede en disposición de aquellos a quienes les pueda beneficiar sin que sea el deseo del propietario. Para esto existen múltiples estándares que podemos seguir o adaptar a nuestro contexto como el **ISO/IEC 27001 ó NMX-I-27001-NYCE-2015.**

Para evitar las situaciones anteriormente mencionadas hice un análisis de los riesgos que existen sobre el manejo de los datos de nuestro socio formador y sus respectivos planes de mitigación:

Esta información fue añadida al documento oficial del equipo.

Riesgos

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

1. Riesgos legales
    1. Violación de acuerdos de confidencialidad
    2. Uso indebido de identificadores oficiales (SINIIGA)
    3. Falta de trazabilidad o registros auditables
    4. Exportación o manejo de datos transfronterizos sin regulación
2. Riesgos técnicos
    1. Pérdida de información
    2. Acceso no autorizado
    3. Filtración de información
    4. Malware o ransomware
3. Riesgos éticos y de privacidad
    1. Uso no autorizado de imágenes (rostros, instalaciones, marcas etc.)
    2. Difusión o publicación sin consentimiento
    3. Falta de consentimiento informado
4. Riesgos operativos
    1. Interrupción del proyecto por incumplimiento de regulaciones

    2. Daño financiero directo por multas, sanciones o litigios
    3. Pérdida de propiedad intelectual
    4. Desconfianza del cliente
5. Riesgos reputacionales e institucionales
    1. Afectación a la marca o institución
    2. Reputación de los colaboradores

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.
    1. Inventariar todos los activos de información (A.5.9 – Inventario de activos de información).
        1. El inventario de los datos y su información relevante se encuentra en Reporte de Data Understanding
    2. Clasificar los datos según su sensibilidad: público, y confidencial (A.5.12 – Clasificación de la información).
        1. 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.
    1. Implementar políticas de acceso mínimo necesario (A.5.15 – Control de acceso).
        1. Los repositorios están únicamente habilitados para profesores y miembros del equipo.
        2. La carpeta de drive del proyecto está únicamente habilitados para profesores y miembros del equipo.
        3. El acceso a las imágenes originales de Queue y Beds está únicamente permitido a los que hicieron la solicitud inicial (Chimali e Imanol)
    2. Autenticación multifactor (A.5.17 – Gestión de credenciales de autenticación).
        1. El acceso a las plataformas github y drive requiere de autenticación multifactor para poder acceder a la información.
    3. Revocación de acceso inmediato al miembro que sea dado de baja del equipo (A.6.3 – Ciclo de vida del acceso del usuario).
        1. Actualmente no se ha suscitado esta situación.
3. Protección física **Mitigación esperada:** minimiza la manipulación o robo físico de activos y equipos.
    1. Restringir el acceso físico a las áreas donde se almacena o procesa información sensible (A.7.4 – Seguridad física).

        1. 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.
    1. Incluir cláusulas de confidencialidad y cumplimiento normativo en los contratos (A.5.19 – Seguridad de la información en relaciones con terceros).
        1. En este documento detallamos las cláusula de confidencialidad y cumplimiento normativo con nuestro cliente: Memorándum de Políticas de Tratamiento y Acceso a Datos
    2. Supervisar el cumplimiento mediante auditorías o revisiones periódicas.
        1. 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.
    1. Capacitar regularmente al personal en temas de protección de datos, phishing, uso responsable de sistemas y cumplimiento legal (A.6.3 – Concientización y formación).
        1. Cada uno de los miembros del equipo leyó conscientemente este documento, participó en su creación y estuvo de acuerdo con lo establecido.
    2. Establecer políticas disciplinarias ante incumplimientos.
        1. 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.
    1. Implementar un sistema de backups (A.8.13 – Copias de seguridad).
        1. Los repositorios que manejamos hace backups automáticamente.
        2. El drive contiene las versiones de los datos a las cuales volver en caso de ser necesario.
        3. Los datos del cliente se encuentran respaldados en un disco duro externo.
    2. Almacenar copias en sitios geográficamente distintos.
        1. 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.
    1. Crear un procedimiento formal de gestión de incidentes (A.5.25 – Gestión de incidentes de seguridad de la información).
        1. 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.
    1. Mantener políticas y procedimientos documentados (A.5.1 – Políticas de seguridad).
        1. Este documento cumple con ese propósito.
    2. NOM-001-SAG/GAN-2015.
        1. 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.
        1.