Instituto de Acuacultura del Estado de Sonora

OFICIO IAES-UT No. 026/2024

Hermosillo, Sonora, 28 de octubre de 2024

C. Roberto Cedano Santibáñez
Correo: cedanosantibanezr@hotmail.com
P R E S E N T E.

En atención a la solicitud de información con número de folio 260490624000026 que hizo llegar por medio del sistema SISAI, a nuestro Organismo, Instituto de Acuacultura del Estado de Sonora "IAES", el día 07 de octubre del presente año, en la que requiere la siguiente información:

Titular de la Unidad de Transparencia:
Con fundamento en lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y su equivalente a nivel estatal, es imperativo que los Responsables del tratamiento y resguardo de datos personales implementen instrumentos que se ajusten a los principios, fundamentos y procedimientos estipulados tanto en las normativas previamente mencionadas como en nuestra Constitución Política.

En virtud de lo anterior, solicito se me proporcione lo siguiente:

1. Análisis de riesgo y brechas: Documentación correspondiente realizada por el Sujeto Obligado.

2. Identificación del encargado: Nombre del funcionario designado para el tratamiento de datos personales, así como una copia de su contrato en versión pública.

3. Listado de medidas de protección: Relación de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos implementados para salvaguardar los datos personales recopilados por su institución.

4. Tratamientos de datos: Listado de los tratamientos a los cuales son sometidos los datos personales en posesión de la institución.

5. Unidad administrativa especializada: Información sobre la existencia de una unidad dedicada a la materia de datos personales,

incluyendo el número de servidores públicos que la conforman, así como sus nombres, niveles y cargos. En caso de no contar con tal unidad, se deberá especificar qué unidad administrativa desempeña estas funciones.

6. Aviso de privacidad: Confirmación de la existencia de un aviso de privacidad, especificando su tipo.

7. Transferencias y remisiones de datos: Número de transferencias y remisiones de datos personales realizadas, en caso de haberse efectuado.

8. Mejores prácticas: Indicación sobre la existencia de esquemas de mejores prácticas implementados en la institución.

Finalmente, reitero que, dado que la información solicitada no implica una recopilación excesiva de datos o documentos, solicito que se me remita a través de los medios digitales disponibles de manera exclusiva.

Me permito hacer de su conocimiento que dicha solicitud ha sido ACEPTADA y se le otorga respuesta.

1.- Análisis de riesgo y brechas: Documentación correspondiente realizada por el Sujeto Obligado.

Respuesta.- Para atender su solicitud de información le informo que estos puntos forman parte del documento de seguridad del Instituto de Acuacultura del Estado de Sonora, en dicho documento se establece que **el Análisis de Riesgos** es una aproximación metódica para determinar el riesgo del tratamiento de los datos personales, siguiendo el siguiente proceso:

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio supondría su degradación
2. Determinar a qué amenazas están expuestos aquellos activos
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza

5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Se presentan los riesgos posibles ante los que se pudiera enfrentar nuestra Entidad.

- Obtención de datos incompletos o incorrectos.
- Omitir la notificación al titular de los datos personales del aviso de privacidad.
- No difundir el aviso de privacidad.
- Ante la necesidad de tener un consentimiento expreso: no tener evidencia de que él o la titular de los datos personales conoce los términos del aviso de privacidad.
- No contar con espacios de almacenamiento seguros y de acceso restringido o contralado, en el cual se puedan archivar y resguardar los expedientes de personal que contengan datos personales sensibles en formato físico.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales.
- Pérdida de expedientes físicos debido a catástrofes, inundaciones, e incendios.
- Daño de la base de datos que contenga información confidencial.
- Fallas técnicas en los equipos de cómputo en donde están las bases de datos.
- Falta de capacitación de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus funciones.
- Pérdida, robo o extravío de expedientes.
- Alteración, modificación, de la información.

A continuación, se relacionan las amenazas identificadas a los sistemas de tratamientos de datos personales del IAES, sus posibles vulneraciones e impactos.

ORIGEN DE LA AMENAZA	CAUSA	POSIBLES CONSECUENCIAS
Acceso de personas no autorizadas a los sistemas o plataformas oficiales del IAES.	Adquirir	Acceso no autorizado, divulgación de datos personales, robo de información, modificaciones no autorizadas y robo de información.
Desconocimiento delpersonal sobre el tratamiento de datos personales	Errores involuntarios y obtención de informaciónpara beneficio personal.	Pérdida de datos personales, uso indebido de datos personales, modificaciones no autorizadas, filtraciones de información o sustracción de datos.
Fallas técnicas.	Pérdida de sistemas, correos electrónicos o plataformas digitales. Equipos tecnológicos dañados o con problemas técnicos.	Daño o pérdida de datos personales, divulgación y transferencias no autorizadas de datos y modificaciones no autorizadas.
Susceptibilidad en equipos, o sistemas.	Falta de contraseñas efectivas, falta de mecanismos para identificar o autentificación de usuarios, falta de	Daño o pérdida de datos personales, divulgación y transferencias no autorizadas de datos y modificaciones no autorizadas.

	actualización de antivirus y sistemas operativos.	
Fallas en la gestión de seguridad.	Procesos y actividades realizadas sin considerar los criterios y lineamientos normativos	Daño o pérdida de datos personales, divulgación y transferencias no autorizadas de datos y modificaciones no autorizadas.
Falta de medidas de seguridad físicas.	Archiveros de fácil acceso, sin llaves para controlar su uso.	Divulgación, alteración, modificación, robo de información realización de transferencias.
Daño y/o alteración de la base de datos que contenga información confidencial.	Falta de un servidor o sistema que almacene los datos personales, falta de registros, bitácoras para regular la entrada y salida del personal autorizado a las áreas de almacenamiento en las que se resguardan los expedientes con datos sensibles.	Daño y/o perdida de los datos personales, modificaciones no autorizadas.
Riesgos de origen humano.	Agua, fuego, accidentes, corrosión, entre otras.	Daño o pérdida de datos personales.
Riesgos de origen natural.	Desastres climatológicos, sismos o cualquier eventualidad de causa natural.	Daño o pérdida de datos personales.

Así como también dar respuesta a dicha solicitud en el paso siguiente de la elaboración del Documento de Seguridad, del Análisis de Riesgo es también el **Análisis de Brecha**, donde debe considerarse lo siguiente:

l. Las medidas de seguridad existente y efectiva;
11. Las medidas de seguridad faltantes, y
111. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles.

El presente análisis identifica el riesgo inherente a los datos personales en los sistemas de tratamiento de las Unidades Administrativas del IAES, la valoración de los riesgos y las medidas de seguridad técnicas, físicas y administrativas.

Una vez identificados los posibles riesgos a los que nuestra Entidad podría ser susceptible de enfrentar, se describen las medidas de seguridad existentes:

- El personal que recaba los datos personales se encuentra adscrito a la unidad administrativa que coordina los sistemas de tratamiento e integra únicamente los datos imprescindibles para cada trámite o servicio.
- El espacio físico o área donde se recaban datos personales, es dentro de las oficinas centrales del Instituto de Acuacultura del Estado de Sonora.
- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.
- En la mayoría de las áreas, el acceso para las personas externas al Instituto está restringido.
- La mayoría de las Unidades Administrativas cuentan con espacios definidos para sus actividades.
- Las llaves de cada área se asignan a personal autorizado por cada una.
- Recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.
- Las llaves de los archiveros con las que se cuentan son asignadas al personal autorizado por la o el Titular de la Unidad Administrativa.
- Recabados los datos personales, si se les da proceso electrónico, el personal responsable de la actividad los guarda en carpeta compartida, correo

electrónico oficial o plataforma.

- Una vez concluido el trámite, los datos personales recabados se resguardan íntegros en la carpeta, archivo o expediente del trámite al que pertenecen.
- Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en el archivo de su Unidad Administrativa.

Las medidas de seguridad que actualmente se realizan son efectivas y deben continuar aplicándose de manera continua y consciente en cada área de este Instituto.

Considerando los sistemas de tratamiento y las medidas de seguridad previamente descritas, para el fortalecimiento de la gestión de seguridad el desarrollo e implementación de medidas es importante incluir las establecidas por la normatividad aplicable, por lo que a continuación se señalan las siguientes medidasde seguridad a implementar al interior de esta Entidad:

- Capacitación continua y permanente en materia de protección de datos personales y normatividad aplicable.
- Implementación de mejoras en el control de consulta física de los expedientes que obran en los archivos de trámite y concentración de las Unidades Administrativas del IAES.
- Capacitación en el proceso de bloqueo y eliminación de datos personales recabados y que por su tiempo concluyen su ciclo de vida.
- Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
- Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.
- Limitar el número de personas con acceso a los archivos físicos.
- Utilizar claves de usuario y contraseñas de manera personal, y evitar socializarlas.
- Utilizar el correo electrónico para fines, relacionados con las actividades laborales evitando remitir datos personales.
- Notificar inmediatamente a la instancia competente los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.

2.- Identificación del encargado: Nombre del funcionario designado para el tratamiento de datos personales, así como una copia de su contrato en versión pública.

El Instituto de Acuacultura del Estado de Sonora, designo a la Lic. Belinda Platt Ávila, como Oficial de Datos Personales según oficio, el cual se adjunta.

3.- Listado de medidas de protección: Relación de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos implementados para salvaguardar los datos personales recopilados por su institución.

Respondiendo a la pregunta le informo que las medidas de seguridad para efectos de resguardo de los datos personales son consideradas según el área donde se realice su trámite, toda vez que se cuenten con medidas de organización y acceso restringido para efecto de que los datos que fueron proporcionados sean utilizados única y exclusivamente para los fines que se mencionan:

- Verificar y confirmar su identidad, así como la autenticidad de la información que nos proporciona para contar con un registro que permita identificar con precisión quién solicita un apoyo, trámite o servicio.
- Acreditar los requisitos necesarios para expedir los documentos sobre los trámites o servicios que ofrece el IAES.
- Realizar trámites administrativos, como el alta de los servidores públicos y actualización de la situación laboral de cada uno, derivado de los constantes movimientos de personal, tales como bajas, licencias, promociones, transferencias, cambios, permuta, reingresos y democión, así como todos los movimientos generados con motivo del servicio, desde su ingreso hasta su baja.
- Acreditar la personalidad para atención a solicitudes para el ejercicio de Derechos ARCO.
- Integrar expedientes y base de datos necesarios para el otorgamiento y operación de los servicios que se contraten, así como las obligaciones que se deriven de los mismos.
- Mantener una base histórica con fines informáticos y/o estadísticos.

Ejemplo de Actividades:

- Evaluaciones de riesgo para identificar vulnerabilidades

- Implementar políticas y procedimientos de seguridad.
- Realización de Auditorías y revisiones regulares
- Mantener actualizados sistemas y software.
- Copias de seguridad
- Bitácoras de Acceso
- Seguridad en Gavetas y escritorios
- Candados

Actividades de Controles de Seguridad en Sistemas o técnicos:

- Firewall
- Antivirus
- Protocolos de Seguridad: https
- Controles de acceso
- Cifrar datos sensibles
- Contraseñas en documentos con datos personales
- Contraseñas en sistemas que utilicen datos personales
- Contraseñas en equipos del personal que utilicen datos personales
- Envío de información con datos personales solo por correos oficiales

En cuanto a medidas administrativas, estamos en espera de agenda con el Órgano Garante para que nos imparta una capacitación en relación al tratamiento datos personales en nuestra Entidad.

4. Tratamientos de datos: Listado de los tratamientos a los cuales son sometidos los datos personales en posesión de la institución.

En nuestra Entidad para el tratamiento de los datos personales se cuenta con el Aviso de Privacidad Integral, el cual se encuentra publicado en nuestra Entidad Instituto de Acuacultura del Estado de Sonora, en el Portal de Sonora Transparente.

5.- Unidad administrativa especializada: Información sobre la existencia de una unidad dedicada a la materia de datos personales, incluyendo el número de servidores públicos que la conforman, así como sus nombres, niveles y cargos. En caso de no contar con tal unidad, se deberá especificar qué unidad administrativa desempeña estas funciones.

El Instituto de Acuacultura no cuenta con la existencia de una Unidad Administrativa especializada en la Protección de Datos Personales, sin

embargo, la Unidad de Transparencia de esta Dependencia es quien desempeña al momento las funciones relacionadas al tema de Datos Personales.

6.- Aviso de privacidad: Confirmación de la existencia de un aviso de privacidad, especificando su tipo.

El aviso de privacidad con el que cuenta el Instituto de Acuacultura del Estado de Sonora es el Aviso de Privacidad Integral, el cual se adjunta en archivo formato PDF.

7.- Transferencias y remisiones de datos: Número de transferencias y remisiones de datos personales realizadas, en caso de haberse efectuado.

En relación a la transferencia y remisiones de datos, después de una consulta con los titulares de cada una de las Unidades administrativas del en el Instituto de Acuacultura del Estado de Sonora, se estableció que la única transferencia de datos que se realiza es la transferencia de expedientes de la recopilación de los trámites administrativos para la contratación de personal, con el fin de darlo de alta como servidor público del Gobierno del Estado de Sonora, por lo tanto el número de transferencias varía dependiendo del personal contratado durante el año en curso.

8.- Mejores prácticas: Indicación sobre la existencia de esquemas de mejores prácticas implementados en la institución.

El Instituto de Acuacultura del Estado de Sonora, es el responsable del uso, protección y tratamiento de sus datos personales, los cuales son protegidos conforme a lo dispuesto por la Ley General de Protección de Datos Personales en posesión de los Sujetos Obligados y de más normatividad aplicable, de tal forma se han implementado mejores prácticas para la protección de los datos personales con la existencia de los Avisos de Privacidad, también según el Programa Anual de Capacitación del año en curso por parte del Órgano Garante se han asistido a capacitaciones relacionadas en el tema de la protección de los datos personales para obtener un continuo conocimiento del tema en mención.

Sin otro particular de momento, quedamos a su disposición.

A T E N T A M E N T E

cDr. RAMON ALBERTO NENNINGER CHECK CINCO
Titular de la Unidad de Transparencia del Instituto de Acuacultura del Estado De Sonora