AGRICULTURA
SECRETARÍA DE AGRICULTURA Y DESARROLLO RURAL

IMIPAS
INSTITUTO MEXICANO DE INVESTIGACIÓN EN PESCA Y ACUACULTURA SUSTENTABLES

DOCUMENTO DE SEGURIDAD DEL INSTITUTO MEXICANO DE INVESTIGACIÓN EN PESCA Y ACUACULTURA SUSTENTABLES (IMIPAS)

ÍNDICE

INTRODUCCIÓN

La Constitución Política de los Estados Unidos Mexicanos en los artículos 6 y 16 reconoce el derecho a la protección de sus datos personales, así como al acceso, rectificación, cancelación y oposición. En relación a dicha disposición, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO o Ley General) establece el conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal que se encuentren en posesión de los sujetos obligados, entre los que se encuentra el Instituto Mexicano de Investigación en Pesca y Acuacultura Sustentables (IMIPAS), Organismo Público Descentralizado de la Administración Pública Federal con personalidad jurídica y patrimonio propio, encargado de dirigir, coordinar y orientar la investigación científica y tecnológica en materia de pesca y acuacultura, así como el desarrollo, innovación y transferencia tecnológica que requiera el sector pesquero y acuícola.

En ese sentido, en cumplimiento a la normatividad aplicable se establece el presente documento de seguridad, definido como el *instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por este Instituto, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee*, mismo que tiene como finalidad *establecer el marco de referencia del tratamiento de los datos personales que se lleva a por las unidades administrativas que lo integran,* así como promover acciones de mejora continua para su protección. Para tales efectos, el IMIPAS ha identificado los procesos que, en el ámbito de su competencia y ejercicio de las atribuciones, involucran el tratamiento de datos personales, a efecto de mantener la seguridad de estos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo con sus respectivos ámbitos de funciones.

Cabe señalar que, los datos personales constituyen el principal activo de información objeto del presente documento, por lo que los elementos que lo integran, constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión del IMIPAS (*sistema de gestión: conjunto de elementos y actividades interrelacionadas para establecer, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales*) el cual permite disponer de manera segura la información relacionada con las medidas de seguridad, el análisis general de las amenazas y posibles vulnerabilidades, así como los mecanismos y/o acciones a implementar para mitigarlas.

Así, el IMIPAS comprometido con la tutela de los datos personales que trata y, acorde a la recomendación emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), ha impulsado a su interior las acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizados a los datos personales, mediante la implementación de medidas físicas, administrativas y técnicas, tendentes a garantizar la seguridad e integralidad de los mismos, su seguimiento y supervisión continuos.

Dicho lo anterior, el presente documento se integra a partir la gestión de actividades coordinadas para controlar y verificar que el tratamiento de los datos personales sea acorde con los principios que rigen su protección, pues para el IMIPAS la política de seguridad en esta materia constituye un compromiso con el cumplimiento de las disposiciones, entre las que se encuentra: Ley General de

Protección de Datos Personales en Posesión de Sujetos Obligados; Ley General de Archivos y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

OBJETIVO Y ALCANCE

Establecer los principales elementos que integran las medidas de seguridad administrativas, físicas y técnicas que ha establecido el IMIPAS para garantizar la confidencialidad, integridad y disponibilidad de los datos personales; así como determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto en un plano general los diverso sistemas de información y procesos en los se tratan datos personales por las diversas unidades administrativas, conforme a lo establecido en la LGPDPPSO y a los Lineamientos Generales de Protección de Datos Personales para el Sector Público; esto con independencia del tipo de sistema en el que se encuentren los datos personales, los cuales deben protegerse contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado.

1. SISTEMA DE GESTIÓN DE LOS DATOS PERSONALES EN POSESIÓN DEL INSTITUTO MEXICANO DE INVESTIGACIÓN EN PESCA Y ACUACULTURA SUSTENTABLES (IMIPAS)

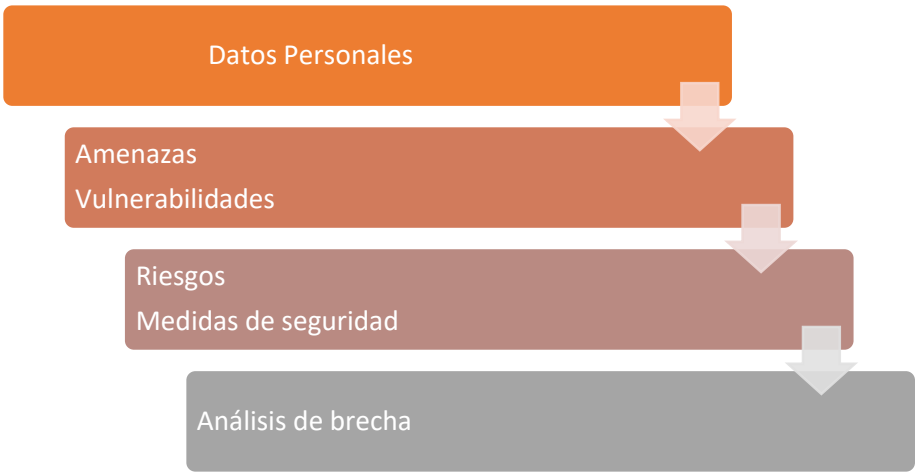
Para el tratamiento de los datos personales que lleva a cabo el IMIPAS a través de su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismos, se establecen políticas y métodos orientados a salvaguardar su confidencialidad, integridad y disponibilidad, en tal virtud, se inició el proceso de planificación de los esquemas de protección de datos mediante la identificación de todos y cada uno de los procesos y tareas en los que se involucra el tratamiento de datos personales, considerando el ámbito de competencia institucional y ejercicio de las atribuciones y/o funciones de las Unidades Administrativas que integran este Instituto, actividad que se refleja en el inventario de datos personales.; el cual ha contribuido desde el punto operativo a considerar el ciclo de vida de los datos personales, de forma tal que los servidores públicos que intervienen en el tratamiento conocen que, una vez concluida la finalidad los datos, éstos deben ser sometidos a un proceso de bloqueo y, en su caso, de cancelación, supresión o destrucción, lo que resulta relevante en el marco del proceso de baja documental.

Asimismo, entre otros aspectos, se identificó la categoría, tipo datos que son sometidos a tratamiento, los medios a través de los cuales se obtienen, el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento; el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento; objeto de la transferencia que en su caso, se realicen y; la identificación de los destinatarios o receptores de los mismos.

De igual forma, conforme a lo establecido en el artículo 33, fracción IV de la Ley General de la materia, se dispuso de la metodología para la elaboración del análisis de riesgos, en la que se identificó el valor de los datos personales de acuerdo con su categoría y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para los titulares de los mismos con motivo de su posible vulneración y, los factores de riesgo a los que eventualmente se encuentran expuestos.

Con base en dicho análisis de riesgo, además de promover el reconocimiento de las medidas de seguridad ***administrativas***, entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; ***físicas***, que corresponden a las acciones o

mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, ***técnicas*** que se valen de la tecnología para proteger el entorno digital de la información, también se han registrado nuevas medidas de seguridad que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados; es decir, el análisis de brecha a partir del cual será posible mitigar los riesgos a los que están expuestos los datos tratados, tal y como se ilustra a continuación el siguiente esquema[1]:



Considerando que la identificación de vulnerabilidades tiene por objeto prevenir posibles dificultades en la seguridad de los datos bajo un enfoque proactivo; es decir, identificar áreas de oportunidad en materia de seguridad de datos personales sin que éstas constituyan un daño efectivo, es que se listan como posibles vulnerabilidades, las siguientes:

- Controles de acceso físico y electrónicos inadecuados a sistemas de archivos.
- Deficiente conocimiento de procedimientos en materia de seguridad de datos.
- Inadecuada administración de autorizaciones de accesos a los datos personales (sistemas de privilegio).
- Falta de definición de perfiles y roles para delimitar funciones manejo y uso de datos.
- Falta de seguimiento y monitoreo a políticas de seguridad.
- Ausencia de mecanismos de confidencialidad por parte del personal (interno) o por terceros (externos).

Aunado a lo anterior, de manera enunciativa más no limitativa, se examinan algunos tipos de amenazas, que pueden ser intencionales o no, a las que podría enfrentarse la institución y sus activos de información.

[1] Integrado con base en el ciclo PHVA, establecido en las Recomendaciones en materia de Seguridad de Datos Personales, publicado por el entonces IFAI, en el DOF el 30 de octubre de 2013, visible en http://dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30%2F10%2F2013

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizado.
- Pérdida o destrucción no autorizada.

Tipos de amenazas

El riesgo que de manera general puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad por parte de las áreas comisionadas están orientadas a proteger los datos personales.

A partir de la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que de acuerdo con la experiencia y mejores prácticas son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento y se determinando como parte del sistema de gestión y política de seguridad institucional. En ese sentido, se indican las reglas generales siguientes:

- Tratar datos personales de manera lícita, esto es, conforme a las disposiciones establecidas por la Ley General;
- Sujetar el tratamiento de los datos personales al principio de consentimiento, salvo las excepciones previstas por la Ley;
- Informar a los titulares del tratamiento de los datos y sus finalidades;
- Procurar que los datos personales tratados sean correctos y estén actualizados;
- Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron;
- Tratar los datos personales estrictamente para propósitos legales o legítimos del IMIPAS
- Limitar el tratamiento de los datos personales al cumplimiento de las finalidades;
- No obtener datos personales a través de medios fraudulentos;
- Respetar la expectativa razonable de privacidad del titular;
- Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades;
- Velar por el cumplimiento de los principios;
- Establecer y mantener medidas de seguridad;
- Guardar la confidencialidad de los datos personales;

- Identificar el flujo y ciclo de vida de los datos personales;
- Mantener actualizado el inventario de datos personales o de las categorías que maneja el IMIPAS;
- Respetar los derechos de los titulares en relación con sus datos personales;
- Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales, y;
- Identificar a los servidores públicos del IMIPAS responsables del tratamiento de los datos personales.

Con base en lo anterior, el IMIPAS determina las pautas de acción del personal encargado de tratamiento de datos personales con miras a generar su correcto resguardo, buscando en todo momento actuar en apego a las directrices de la LGPDPPSO y los Lineamientos de la materia, siempre en consideración de la salvaguarda del derecho a la privacidad y protección de datos de las personas.

2. INVENTARIO DE DATOS PERSONALES DEL INSTITUTO MEXICANO DE INVESTIGACIÓN EN PESCA Y ACUACULTURA SUSTENTABLES (IMIPAS)

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el Instituto Mexicano de Investigación en Pesca y Acuacultura Sustentables (IMIPAS) elabora de manera permanente un inventario de datos personales con la información básica por cada tratamiento de datos personales.

Esto último de acuerdo al artículo 35, fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y, artículos 58 y 59 de los *Lineamientos Generales de Protección de Datos Personales para el Sector Público*, en donde se dispone elaborar un inventario de datos personales y de los sistemas de tratamiento, tomando en cuenta el contexto en el que ocurren los tratamientos y su ciclo de vida (*obtención, uso y posterior supresión)*.

Contratación de Servicios Profesionales	
Unidad Administrativa responsable	Subdirección de Recursos Materiales
Medio (físico y/o electrónico) por el cual se obtiene el dato personal	Físico y/o electrónico
Datos personales que se solicitan	Datos personales de los Prestadores de Servicios Profesionales RFC, CURP, DOMICILIO, ACTA DE NACIMIENTO, COMPROBANTE DE ESTUDIOS, GÉNERO, NOMBRE, IDENTIFICACIÓN
Finalidad del tratamiento del dato personal	Realizar la contratación del servicio
Datos personales sensibles que se solicitan (en caso de solicitar)	No se solicitan datos personales sensibles
Ubicación física y/o electrónica del dato personal	Archivo de Concentración y electrónicos
Servidor o servidores públicos que tienen acceso al dato personal	Subdirector de Recursos Materiales
Fundamento jurídico del tratamiento	Ley Federal de Transparencia y Acceso a la Información Pública, Ley General de

	Transparencia y Acceso a la Información Pública, Ley General de Archivo, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, Manual de Organización del Instituto Nacional de Pesca (*actualmente IMIPAS)*
Remisiones y/o transferencias (en caso de que se transfiera el dato personal a terceros)	No se realizan transferencias de datos personales, salvo aquellas que sean necesarias para atender requerimientos de información de una autoridad competente.
Integración de expedientes del personal	
Unidad Administrativa responsable	Subdirección de Recursos Humanos
Medio (físico y/o electrónico) por el cual se obtiene el dato personal	Físico y/o electrónico
Datos personales que se solicitan	Nombre, INE, CURP, RFC, Acta de Nacimiento, Cartilla del Servicio Militar, Constancia de Situación Fiscal, Constancia de no inhabilitación, CV, Comprobante de estudios, Cédula profesional, Comprobante de Domicilio, Número de cuenta bancaria, Número de celular o de casa, Correo electrónico, Fotografía
Finalidad del tratamiento del dato personal	Integración del expediente personal; alta de la persona en la nómina y para el llenado de seguros institucionales.
Datos personales sensibles que se solicitan (en caso de solicitar)	No se requieren datos personales sensibles
Ubicación física y/o electrónica del dato personal	Ubicación física: En la dependencia, Avenida Cuauhtémoc #1230, Santa Cruz Atoyac, Benito Juárez, 03310, Ciudad de México, México. Ubicación electrónica: En la computadora del área.
Servidor o servidores públicos que tienen acceso al dato personal	Subdirectora de Recursos Humanos, Jefe de Departamento.
Fundamento jurídico del tratamiento	Manual de Organización Instituto Nacional de Pesca y Acuacultura; Estatuto Orgánico; Ley General de Transparencia y Acceso a la Información Pública, Ley General de Protección de Datos Personales en posesión de sujetos obligados.
Remisiones y/o transferencias (en caso de que se transfiera el dato personal a terceros)	ISSSTE, Plataforma Nacional de Transparencia.
Solicitudes de acceso a la información y de ejercicio de derechos ARCO	

Unidad Administrativa responsable	Unidad de Transparencia del Instituto Mexicano de Investigación en Pesca y Acuacultura Sustentable
Medio (físico y/o electrónico) por el cual se obtiene el dato personal	Electrónico.
Datos personales que se solicitan	Nombre, domicilio, correo electrónico, teléfono, nombre del representante, documentos para identificar la identidad del titular o del representante legal y descripción de la solicitud.
Finalidad del tratamiento del dato personal	Documentar, registrar, dar seguimiento y brindar respuesta a las solicitudes de acceso a la información y de protección de datos personales, a través del ejercicio de los derechos de acceso, rectificación, cancelación y oposición a su tratamiento.
Datos personales sensibles que se solicitan (en caso de solicitar)	No se solicitan datos personales sensibles
Ubicación física y/o electrónica del dato personal	Plataforma Nacional de Transparencia administrada por personal de la Unidad de Transparencia.
Servidor o servidores públicos que tienen acceso al dato personal	Servidores públicos integrantes del Comité de Transparencia.
Fundamento jurídico del tratamiento	Artículo 45, fracción VIII de la Ley General de Transparencia y Acceso a la Información Pública; diverso 61 de la Ley Federal de Transparencia y Acceso a la Información Pública; 4, 16 a 18, 20 a 42 y, 57, 85, fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás relativos y aplicables.
Remisiones y/o transferencias (en caso de que se transfiera el dato personal a terceros)	No se realizan transferencias de datos personales, salvo aquellas que sean necesarias para atender requerimientos de información de una autoridad competente.

3.- FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

Las personas servidoras públicas del IMIPAS, responsables de realizar tratamientos de datos personales, deberán:

1. Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en la obtención y tratamiento de datos personales, documentando el cumplimiento de estos principios en el ejercicio de sus funciones.

2. Privilegiar en todo momento, la protección de los intereses del titular de los datos personales.

3. Tratar los datos personales en el marco estricto de las facultades o atribuciones que la normatividad aplicable le confiera en el ejercicio de sus cargos y funciones.

4. Verificar a través de la expresión documental correspondiente, que previo al tratamiento de los datos personales, se obtuvo el consentimiento tácito, expreso o expreso por escrito del titular.

5. Las personas servidoras públicas responsables, deberán elaborar y actualizar el aviso de privacidad en sus modalidades integral y simplificado cuando las características del tratamiento que efectúan lo requieran y garantizarán la difusión de estos. En el caso de Aviso de Privacidad Integral, supervisará que se encuentre publicado de manera actualizada en el Apartado Virtual de Protección de Datos Personales del IMIPAS.

6. Para cumplimiento del deber de seguridad, deberá implementar a través de un Programa de Trabajo, las medidas físicas, técnicas y administrativas descritas en el presente Documento de Seguridad y colaborará en la elaboración y actualización de los respectivos análisis de riesgos y de brecha. Asimismo, en seguimiento a las tareas descritas en el Sistema de Gestión, aplicará los mecanismos para monitorear y revisar la aplicación de las medidas descritas documentando los resultados.

7. Para cumplimiento del deber de confidencialidad, las personas servidoras públicas responsables, deberán suscribir las cartas respectivas de confidencialidad que se instrumentarán a través de la Coordinación Administrativa correspondiente.

4. ANÁLISIS DE RIESGOS

Se protege la información relacionada con el análisis de riesgo y de brecha, en atención a lo establecido en la Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia, que forma parte de los instrumentos técnicos aprobados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante Acuerdo ACT-PUB/17/11/2021.05, de fecha 17 de noviembre de 2021 y publicado en el Diario Oficial de la Federación el 26 de noviembre de 2021.

En la referida Metodología se establece en la Vertiente 2: Deberes, Variable 2.1: Deber de seguridad, Criterio 1 del Formato 2.1 y en la Vertiente 4: Portabilidad, Variable 4.1: Portabilidad de datos personales, Criterio 6 del Formato 4.1.

"... Por ningún motivo debe incluirse en este apartado el documento de seguridad integro con el que cuenta el responsable. El documento de seguridad deberá publicarse protegiendo el plan de trabajo, el análisis de riesgo y el análisis de brecha respectivos; lo que implica que en caso de que se dejen visibles, sin excepción, será considerado como incumplimiento al presente criterio. ..."

5. ANÁLISIS DE BRECHA

Se protege la información relacionada con el análisis de riesgo y de brecha, en atención a lo establecido en la Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia, que forma parte de los instrumentos técnicos aprobados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante Acuerdo ACT-PUB/17/11/2021.05, de fecha 17 de noviembre de 2021 y publicado en el Diario Oficial de la Federación el 26 de noviembre de 2021.

En la referida Metodología se establece en la Vertiente 2: Deberes, Variable 2.1: Deber de seguridad, Criterio 1 del Formato 2.1 y en la Vertiente 4: Portabilidad, Variable 4.1: Portabilidad de datos personales, Criterio 6 del Formato 4.1.

"... Por ningún motivo debe incluirse en este apartado el documento de seguridad integro con el que cuenta el responsable. El documento de seguridad deberá publicarse protegiendo el plan de trabajo, el análisis de riesgo y el análisis de brecha respectivos; lo que implica que en caso de que se dejen visibles, sin excepción, será considerado como incumplimiento al presente criterio. ..."

6. PLAN DE TRABAJO

Se protege la información relacionada con el análisis de riesgo y de brecha, en atención a lo establecido en la Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia, que forma parte de los instrumentos técnicos aprobados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante Acuerdo ACT-PUB/17/11/2021.05, de fecha 17 de noviembre de 2021 y publicado en el Diario Oficial de la Federación el 26 de noviembre de 2021.

En la referida Metodología se establece en la Vertiente 2: Deberes, Variable 2.1: Deber de seguridad, Criterio 1 del Formato 2.1 y en la Vertiente 4: Portabilidad, Variable 4.1: Portabilidad de datos personales, Criterio 6 del Formato 4.1.

"... Por ningún motivo debe incluirse en este apartado el documento de seguridad integro con el que cuenta el responsable. El documento de seguridad deberá publicarse protegiendo el plan de trabajo, el análisis de riesgo y el análisis de brecha respectivos; lo que implica que en caso de que se dejen visibles, sin excepción, será considerado como incumplimiento al presente criterio. ..."

Se protege la información relacionada con el análisis de riesgo y de brecha, en atención a lo establecido en la Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia, que forma parte de los instrumentos técnicos aprobados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante Acuerdo ACT-PUB/17/11/2021.05, de fecha 17 de noviembre de 2021 y publicado en el Diario Oficial de la Federación el 26 de noviembre de 2021.

En la referida Metodología se establece en la Vertiente 2: Deberes, Variable 2.1: Deber de seguridad, Criterio 1 del Formato 2.1 y en la Vertiente 4: Portabilidad, Variable 4.1: Portabilidad de datos personales, Criterio 6 del Formato 4.1.

"... Por ningún motivo debe incluirse en este apartado el documento de seguridad integro con el que cuenta el responsable. El documento de seguridad deberá publicarse protegiendo el plan de trabajo, el análisis de riesgo y el análisis de brecha respectivos; lo que implica que en caso de que se dejen visibles, sin excepción, será considerado como incumplimiento al presente criterio. ..."

Se protege la información relacionada con el análisis de riesgo y de brecha, en atención a lo establecido en la Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia, que forma parte de los instrumentos técnicos aprobados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, mediante Acuerdo ACT-PUB/17/11/2021.05, de fecha 17 de noviembre de 2021 y publicado en el Diario Oficial de la Federación el 26 de noviembre de 2021.

En la referida Metodología se establece en la Vertiente 2: Deberes, Variable 2.1: Deber de seguridad, Criterio 1 del Formato 2.1 y en la Vertiente 4: Portabilidad, Variable 4.1: Portabilidad de datos personales, Criterio 6 del Formato 4.1.

"... Por ningún motivo debe incluirse en este apartado el documento de seguridad integro con el que cuenta el responsable. El documento de seguridad deberá publicarse protegiendo el plan de trabajo, el análisis de riesgo y el análisis de brecha respectivos; lo que implica que en caso de que se dejen visibles, sin excepción, será considerado como incumplimiento al presente criterio. ..."

7. MEDIDAS DE SEGURIDAD

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta el Instituto Mexicano de Investigación en Pesca y Acuacultura Sustentables (IMIPAS) para mantener la confidencialidad e integralidad de la información, así como para proteger los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada, son las siguientes:

Medidas administrativas

1. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.
2. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes.
3. Mecanismos de control desarrollados conforme a lo establecido en los lineamientos del Sistema de Gestión de Documentos institucional.
4. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
5. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

Medidas físicas

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.
2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.
3. Limitar el número de personas con acceso a archivos físicos.
4. Realizar el registro de personas con acceso a espacios físicos en los que se resguarda información con datos personales.
5. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.
6. Resguardo de llaves en oficinas de acceso restringido.

Medidas técnicas

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registradas a la vista de otras personas.
2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o

descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.

3. Notificar de manera inmediata al Departamento de Tecnologías de la Información y Comunicaciones los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.
4. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.
5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.
6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.
7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.
8. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.
9. Borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que nos son necesarios para el desarrollo de funciones.
10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

8. MONITOREO DE MEDIDAS DE SEGURIDAD

La supervisión de las medidas de seguridad técnicas y físicas es un elemento importante para la mejora continua, pues permite definir nuevos controles de monitoreo y seguimiento de éstas. Entre las medidas de supervisión y monitoreo se encuentran las siguientes:

1. Revisar la actualización permanente del esquema de contraseñas conforme a las pantallas de parametrización de los sistemas, verificando que los valores se encuentren determinados conforme a la política.
2. Monitorear que todas las cuentas que se dan de alta para otorgar acceso a la red, sea validada en el campo correspondiente a la contraseña, a fin de asegurar el uso.
3. Revisar el cumplimiento de protocolos.
4. Validar que los accesos, baja o cambio a sistemas se realicen conforme al proceso de administración de usuarios.
5. Vigilar que el ingreso de personas sea a través de los accesos correspondientes, plenamente identificados.

9. PROPUESTA DE CAPACITACIÓN EN MATERIA DE DATOS PERSONALES

De acuerdo con el artículo 30 de la Ley General de Protección de Datos Personales y Posesión de Sujetos Obligados, uno de los mecanismos que el responsable para cumplir con el principio de Responsabilidad, establecido en la mencionada Ley es la puesta en práctica de un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.

Asimismo, el artículo 48 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, menciona que el responsable deberá establecer anualmente un programa de

capacitación y actualización en materia de protección de datos personales dirigidos a su personal y a encargados, el cual deberá ser aprobado, coordinado y supervisado por su Comité de Transparencia.

La elaboración del Programa de Capacitación del Instituto Mexicano de Investigación en Pesca y Acuacultura Sustentables (IMIPAS), asegura el desarrollo de aptitudes, habilidades y responsabilidades de cada servidor público en materia de transparencia, acceso a la información y protección de datos personales y considera el fortalecimiento de competencias éticas para fomentar en las personas servidoras públicas responsables, la concientización en la importancia y valor social que tiene la transparencia, el acceso a la información, la rendición de cuentas la apertura gubernamental, para fortalecimiento de sociedades y gobiernos democráticos.

De manera resumida, las acciones de capacitación en materia de protección de datos personales abordan incluyen los temas: Políticas de acceso a la información; Interpretación y argumentación jurídica; Introducción a la Ley General de Archivos; Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública; Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; Ética Pública y; Clasificación de la Información y Prueba de Daño.

10. ACTUALIZACIÓN

El presente documento de seguridad se encuentra sujeto a modificaciones recurrentes, en tanto que se busca la mejora continua en materia de seguridad de los datos personales. Por ello, una vez elaborado, deberá conocerse que hay supuestos por los cuales dicho documento debe ser actualizado conforme a los establecido al artículo 36 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el cual menciona que el responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos: Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo; Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión; Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida e; Implementación de las acciones correctivas y preventivas ante una vulneración de seguridad.

LIC. ROBERTO SOLIS GARDUÑO

PRESIDENTE

MTRA. JESSICA BERENICE PENILLA CORTÉS

TITULAR DEL ÁREA DE ESPECIALIDAD EN CONTROL INTERNO EN EL RAMO AGRICULTURA Y DESARROLLO RURAL, EN SUPLENCIA DE LA PERSONA TITULAR DEL ÓRGANO ESPECIALIZADO EN CONTROL INTERNO

LIC. DANTE JUÁREZ DURÁN

SUBDIRECTOR DE RECURSOS MATERIALES