DOCUMENTO DE SEGURIDAD DEL FONDO DE CAPITALIZACIÓN E INVERSIÓN DEL SECTOR RURAL (FOCIR)

Ciudad de México a 31 de mayo de 2024

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

Contenido

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

PRESENTACIÓN

La Constitución Política de los Estados Unidos Mexicanos, en su artículo 6°, inciso A, establece que:

> ***II*** *La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.*
>
> ***III*** *Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.*

Por otra parte, el artículo 16 constitucional establece, en su segundo párrafo:

> *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante, la LGPDPPSO), tiene como objeto establecer el derecho que tiene toda persona a la protección de sus datos personales, que estén en posesión de los sujetos obligados.

Dentro de las obligaciones previstas se encuentra el deber de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, detección o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

La LGPDPPSO dispone que el tratamiento de datos personales que realicen los sujetos obligados estará regido por ocho principios y dos deberes: licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad; mientras que los dos deberes son el de confidencialidad y seguridad. Estos principios, deberes y derechos imponen obligaciones para los sujetos obligados, cuya finalidad es que el tratamiento se realice garantizando la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de los titulares.

OBJETIVO

De conformidad con el artículo 35 de la LGPDPPSO, el Documento de Seguridad del Fondo de Capitalización e Inversión del Sector Rural (FOCIR), tiene por objetivo establecer las medidas de seguridad administrativas, físicas y técnicas mínimas que deberán observar quienes realicen el tratamiento de los datos personales que se encuentren en posesión de este Sujeto Obligado; así como el plan de trabajo y de capacitación necesario para garantizar la óptima protección de los datos personales que se encuentran en su poder.

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

El Documento de Seguridad consta de los siguientes apartados:

- Objetivo.
- Inventarios de datos personales.
- Funciones y obligaciones de las personas que tratan datos personales.
- Análisis de Riesgos.
- Análisis de brecha y Plan de Trabajo.
- Programa General de Capacitación.

En ese sentido, en cumplimiento de las obligaciones antes descritas, a continuación, se presenta el documento de seguridad del FOCIR con los elementos informativos que establece el artículo 35 de la LGPDPPSO el cual es de observancia obligatoria para las personas servidoras públicas que realicen algún tipo de tratamiento de datos personales.

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

Inventario de datos personales

Para poder verificar el cumplimiento de las obligaciones previstas en los artículos 33, fracción III y 35, fracción I de la LGPDPPSO y, 58 y 59 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, el FOCIR elaboró los inventarios de datos personales de las unidades administrativas del Fondo.

Sobre el particular, los artículos 58 y 59 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (en lo sucesivo, los Lineamientos Generales) establecen lo siguiente:

Inventario de datos personales
Artículo 58. Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:

I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
II. Las finalidades de cada tratamiento de datos personales;
III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento; En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y
VI. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

Ciclo de vida de los datos personales en el inventario de éstos
Artículo 59. Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:

I. La obtención de los datos personales;
II. El almacenamiento de los datos personales;
III. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
V. El bloqueo de los datos personales, en su caso, y
VI. La cancelación, supresión o destrucción de los datos personales

El responsable deberá identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.

A partir de lo anterior, el FOCIR elaboró los inventarios de los tratamientos de datos personales que realiza, identificando los elementos informativos que señala el artículo 58 de los Lineamientos Generales y basados en el ciclo de vida de los mismos, así como lo requiere el artículo 59 de los Lineamientos Generales, definiéndose de la siguiente manera:

ÁREA ADMINISTRATIVA	TRATAMIENTO DE DATOS PERSONALES	NOMBRE DEL TRATAMIENTO
Dirección Jurídica	1	Suscripción de convenios
Unidad de Género	1	Uso de la ludoteca
Unidad de Transparencia	1	Atención a su solicitud de ejercicio de derechos ARCO
Dirección de Recursos Humanos y Materiales	5	Videovigilancia Procedimiento de Adquisiciones, Arrendamientos y Servicios Contratación del Personal del FOCIR Procedimientos de Enajenación de Bienes Muebles Estudio de Mercado
Dirección de Inversión en Fondos de Capital Privado	1	Inversión en Fondos de Capital Privado
Dirección de Promoción de Banca de Inversión	1	Promoción de Banca de Inversión
Unidad de Operación de Programas Sectoriales	1	Programas apoyados

Las funciones y obligaciones de las personas que traten datos personales

El artículo 33, fracción II de la LGPDPPSO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la definición de las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

Como se señaló, de acuerdo con la fracción II del artículo 35 de la LGPDPPSO, este elemento informativo forma parte del documento de seguridad.

Sobre el particular, el artículo 57 de los Lineamientos Generales señala lo siguiente:

> ***Funciones y obligaciones***
> ***Artículo 57.***
> ***Con relación a lo dispuesto en el artículo 33, fracción II de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.***
>
> ***El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento***

Para ello, el responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.

De conformidad con lo anterior, se establecieron al interior de las unidades administrativas del FOCIR, las funciones, obligaciones y roles del personal que trata datos personales.

Para ello se identificaron dos niveles:

a) Específicos. Cada inventario contempla un apartado exclusivo para que de manera precisa se indique las personas servidoras públicas que realizan el tratamiento, su área de adscripción y el tratamiento específico que realizan.

PERSONAS SERVIDORAS PÚBLICAS QUE TIENEN ACCESO A LA BASE DE DATOS	ÁREA DE ADSCRIPCIÓN	FINALIDAD DE ACCESO	ROL
Señalar los puestos de las personas servidoras públicas que tienen acceso a la base de datos del tratamiento correspondiente (uno por fila)	Definir unidad administrativa a la que está adscrito el puesto	Señalar con que fines tienen acceso las personas servidoras públicas antes identificados (uno por fila)	Responsable de acuerdo con sus funciones y responsabilidades.

El área responsable verificó que las personas servidoras públicas cuenten con atribuciones para ello, de conformidad con el Manual de Organización del FOCIR.

b) Generales. Cualquier persona que realice el tratamiento de datos personales al interior del FOCIR, deberá:

1. Verificar que el tratamiento que realice se encuentre reportado en el inventario respectivo. De no encontrarse reportado, deberá avisar a su superior jerárquico y a la Unidad de Transparencia.
2. Verificar de forma regular que el inventario que documenta el tratamiento que realiza, así como los avisos de privacidad integrales y simplificados, se encuentren actualizados.
3. Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, en el tratamiento de datos personales.
4. Recabar el consentimiento para el tratamiento de los datos personales cuando proceda.
5. Capacitarse de manera constante en materia de protección de datos personales.

TIPO DE MANDOS	OBLIGACIONES PARA EL TRATAMIENTO DE DATOS PERSONALES
Mandos superiores	Supervisar el tratamiento realizado, así como acercarse con las unidades en caso de considerar que las medidas de seguridad implementadas sean las necesarias para garantizar la integridad de los datos personales. Llevar el control de alta y baja de las personas servidores públicas que puedan tener acceso a los datos personales en tratamiento.
Mandos Medios	Coadyuvar en la actualización de registros de las personas servidoras públicas que realizan tratamiento; así como solicitar la cancelación de los permisos respectivos cuando una persona deje laborar para el FOCIR.
Nivel Operativos	Conocer las medidas de seguridad que debe implementar al tratar los datos personales y verificar que, medidas tomar en casi de vulnerar los datos personales.

Análisis de riesgos, Análisis de brecha y Plan de Trabajo

El artículo 33, fracciones IV, V y VI de la LGPDPPSO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización del análisis de riesgo, análisis de brecha y plan de trabajo, en los siguientes términos:

Artículo 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

I. […]
IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;
V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;
[…]

Como se señaló, de acuerdo con las fracciones III, IV y V del artículo 35 de la LGPDPPSO, los análisis de riesgo y brecha y el plan de trabajo forman parte del documento de seguridad.
Por su parte, los artículos 60, 61 y 62 de los Lineamientos Generales establecen lo siguiente:

Análisis de riesgos
Artículo 60. Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;
III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
V. Los factores previstos en el artículo 32 de la Ley General.

Análisis de brecha
Artículo 61. Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:

I. Las medidas de seguridad existentes y efectivas;
II. Las medidas de seguridad faltantes, y

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Plan de trabajo
Artículo 62. De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Por su parte, el artículo 32 de la LGPDPPSO, citado en la fracción V del artículo 60 de los Lineamientos Generales, dispone lo siguiente:

Artículo 32. Las medidas de seguridad adoptadas por el responsable deberán considerar:

I. El riesgo inherente a los datos personales tratados;
II. La sensibilidad de los datos personales tratados;
III. El desarrollo tecnológico;
IV. Las posibles consecuencias de una vulneración para los titulares;
V. Las transferencias de datos personales que se realicen;
VI. El número de titulares;
VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Análisis de riesgos

A partir de lo dispuesto por los artículos antes citados, las unidades administrativas del FOCIR realizaron sus análisis de riesgo, con el objetivo de localizar y visualizar los recursos materiales, técnicos y humanos relacionados con el tratamiento que realizan y que están más expuestos a sufrir un daño por algún impacto negativo, para tomar acciones o medidas adecuadas para atender las vulnerabilidades y/o amenazas. Para evaluar los riegos, las unidades administrativas consideraron todos los posibles escenarios en los que se haría efectivo.

El análisis, consideró el ciclo de vida de datos personales (obtención, uso, almacenamiento, transferencia, eliminación y archivo).

A través de este análisis se determinaron los riesgos de mayor impacto que podrían tener los datos personales tratados, tomando en cuenta las amenazas y vulnerabilidades existentes que afectan la integridad, confidencialidad y disponibilidad de los mismos, con el fin de que las unidades administrativas, reconozcan, analicen, prioricen y adopten los controles y/o medidas de seguridad a implementar.

De forma general, el riesgo atiende a la combinación de la probabilidad de que por una vulneración ocurra una amenaza y de sus consecuencias desfavorables; de modo que, al determinar los riesgos del FOCIR, se podrá realizar un estimado de las medidas de seguridad

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

necesarias para preservar la información personal, mediante trabajos constantes de mejora continua.

Metodología para el análisis de riesgos

Es importante tener en claro que no existe el riego cero, es decir, el riesgo no se podrá erradicar completamente, pero sí minimizar a través de la mejora continua.

La seguridad de los datos personales se basa en el entendimiento de la naturaleza de los riesgos al que están expuestos. El riesgo atiende a la combinación de la probabilidad de que una vulneración ocurra y las consecuencias desfavorables que genere, de modo tal que, al determinar el riesgo en el escenario del FOCIR, se puede evaluar el impacto y así realizar un estimado de las medidas de seguridad necesarias para preservar la información personal.

Riesgo= Probabilidad de Amenaza x Impacto

En este contexto, los elementos que utilizaron las unidades administrativas para analizar los riesgos de los recursos involucrados en el tratamiento de datos personales fueron:

Identificación de activos

Un activo es un recurso (ya sea material o físico, como documentos, servicios, prácticas, políticas, instalaciones; técnico como *software* o *hardware*, o humano como personas, etc.) que tiene valor para el FOCIR y necesite, por tanto, ser protegido de potenciales riesgos.

Los activos evaluados fueron aquéllos que se encontraban relacionados con el ciclo de vida de los datos personales previamente identificados y sus distintos tratamientos.

De acuerdo con los Lineamientos Generales de Datos se pueden identificar tres tipos de activos de apoyo:

Técnicos:

- *Hardware* (equipo de procesamiento de datos como computadoras, servidores, equipo móvil, periféricos);
- *Software* (sistemas operativos como CPU, memoria, discos, procesos, aplicaciones, sistemas de servicio como antivirus, paquetería de software, administradores de bases de datos, mensajería instantánea, servidores web);
- Redes y Telecomunicaciones (medios y equipos);
- Soportes electrónicos (discos ópticos como CD'S y DVD'S, cintas de audio, videos y datos, discos duros removibles, memorias USB);

Material:

- Papel escrito a mano o impreso, transparencias, fotografías, expedientes, documentos;
- Infraestructura adicional (edificios, coches, instalaciones, etc.);
- Estructura organizacional (políticas, servicios, prácticas);

Humanos:

- Personal (servidoras y servidores públicos adscritos al FOCIR, transferentes y receptores, encargados, titulares, contratistas, terceros).

Identificador de amenazas

Para que algo pueda ser considerado amenaza, debe tener el potencial de dañar un activo y causar una vulneración a la seguridad. Las amenazas pueden ser de origen natural y humano, accidentales o deliberadas y provenir de adentro o afuera del FOCIR.
Las amenazas se identificaron considerando que algunas pudieran afectar a más de un activo en el mismo tiempo.

Amenazas comunes

Tipo	Amenaza	Origen
Daño físico	Fuego accidental	Deliberado, ambiental
	Daños por agua	Accidental, deliberado, ambiental
	Contaminación accidental	Deliberado, ambiental
	Accidente grave	Accidental, deliberado, ambiental
	Destrucción de equipos o medios	Accidental, deliberado, ambiental
	Polvo, corrosión congelación	Accidental, deliberado, ambiental
Eventos naturales	Fenómeno climático	Ambiental
	Fenómeno sísmico	Ambiental
	Fenómeno volcánico	Ambiental
	Fenómeno meteorológico	Ambiental
	Inundación por fuerza natural	Ambiental
Perdida de servicios esenciales	Fallo del sistema de suministro de agua o aire acondicionado	Deliberado, ambiental
	Pérdida de suministro de energía	Accidental, deliberado, ambiental
	Fallo del equipo de telecomunicaciones	Deliberado, ambiental
Perturbación debido a radiación	Radiación electromagnética	Accidental, deliberado, ambiental
	Radiación termal	Accidental, deliberado, ambiental
	Pulsos electromagnéticos	Accidental, deliberado, ambiental
Información comprometida	Intercepción de señales de interferencia comprometedoras	Deliberado
	Espionaje remoto	Deliberado
	Escuchar deliberadamente a escondidas	Deliberado
	Robo de soportes o documentos	Deliberado
	Robo de equipo	Deliberado
	Recuperación de medios reciclados o desechados	Deliberado
	Divulgación	Deliberado
	Datos de fuentes no confiables	Deliberado, ambiental
	Manipulación de hardware	Deliberado
	Manipulación de Software	Deliberado, ambiental
	Detección de posición	Deliberado
Fallas técnicas	Falla en el equipo	Ambiental
	Mal funcionamiento del equipo	Ambiental

Tipo	Amenaza	Origen
	Saturación del sistema de información	Deliberado, ambiental
	Mal funcionamiento de software	Ambiental
	Incumplimiento del mantenimiento del sistema de información	Deliberado, ambiental
Acciones no autorizadas	Uso no autorizado de equipos	Deliberado
	Copia fraudulenta de software	Deliberado
	Uso de Software falsificado o copiado	Deliberado, ambiental
	Corrupción de datos	Deliberado
	Tratamiento ilegal de datos	Deliberado
Compromiso de funciones	Error en uso	Ambiental
	Abuso de derechos	Deliberado, ambiental
	Forja de derechos	Deliberado
	Negación de acciones	Deliberado
	Incumplimiento de disponibilidad de personal	Accidental, deliberado, ambiental

Probabilidad de que ocurra una amenaza

No todas las amenazas tienen la misma posibilidad de ocurrencia, debido a que habrá algunas que su presencia sea remota y otras que la probabilidad pueda ser alta. Por cada amenaza, las unidades administrativas, con base en su experiencia y conocimiento de los activos, consideraron la probabilidad de ocurrencia.

Identificación de vulnerabilidades

Las vulnerabilidades son debilidades en la seguridad de los activos. Pueden existir casos en que las vulnerabilidades no se encuentren expuestas a una amenaza identificada y que posiblemente no requieran la implementación de un control, sin embargo, si deben estar perfectamente reconocidas y monitoreadas constantemente, revisando cualquier cambio.

Las medidas de seguridad usadas incorrectamente o con una mala implementación son una causa de vulnerabilidad. Una medida puede ser efectiva o no, dependiendo del contexto en el cual opera. Las vulnerabilidades pueden estar relacionadas a propiedades de los activos que a su vez pueden ser usadas para propósitos distintos a los que se habían destinado originalmente.

Estimado del impacto a los activos a través de la identificación del posible daño (evaluación del riesgo)

Para el análisis de riesgo se evaluó el estimado del impacto a los activos, con mediciones de muy bajo, bajo, medio, alto o muy alto, así como la identificación del posible daño (Riesgo Inherente).

Se determinó el daño que el riesgo pudiera causar a los activos, si era tolerable o debía mitigarse, de conformidad con el artículo 38 de la LGPDPPSO y los supuestos de vulneración:

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

En la elaboración del análisis de riesgo fue esencial conocer el valor o relevancia de los datos personales, así como de los activos involucrados en su tratamiento para establecer en orden de prioridad la atención a los riesgos que se identificaron.

Análisis de Brecha

El análisis de brecha consiste en identificar la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.

Para ello las unidades administrativas del FOCIR definieron las brechas existentes, e identificaron soluciones para reducir, mitigar o aceptar el riesgo, y, por tanto, garantizar una protección integral de los datos personales.

La identificación de la brecha permitirá identificar los alcances para obtener la solución, planeando como y con que se va a cerrar esa brecha para lograr el objetivo.

Para ello, una vez que se contó con el inventario de datos personales, la información de las medidas de seguridad implementadas por las diversas áreas administrativas, el análisis de riesgo revisado y validado por las áreas administrativas que centralizan la protección física y técnica de datos y la revisión de todos los insumos, se definieron las medidas que se encuentran pendientes de implementación para eliminar y matizar los riesgos detectados.

Es importante señalar que derivado de este análisis se detectaron cuáles son los controles (o medidas de seguridad), así como las medidas identificadas como faltantes, para construir un programa de trabajo que refleje las expectativas a lograr, las áreas administrativas involucradas y las fechas compromisos para su implementación.

Plan de Trabajo

Una vez realizados los análisis de riesgo y brechas, se elaboró un plan de trabajo, con la finalidad de implementar las medidas de seguridad más relevantes inmediatas a establecer, así como para el cumplimiento cotidiano de las políticas de tratamiento de los datos personales; priorizando las medidas de seguridad más relevantes e inmediatas a establecer, así como el tipo de medida de seguridad, recomendación, áreas involucradas, expectativa y fecha de cumplimiento.

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

Mecanismos de monitoreo y revisión de las medidas de seguridad

El artículo 33, fracción VII de la LGPDPPSO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

> ***Monitoreo y supervisión periódica de las medidas de seguridad implementadas***
> ***Artículo 63. Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.***
>
> ***Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:***
>
> ***I. Los nuevos activos que se incluyan en la gestión de riesgos;***
> ***II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;***
> ***III. Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;***
> ***IV. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;***
> ***V. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;***
> ***VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y***
> ***VII. Los incidentes y vulneraciones de seguridad ocurridas.***
>
> ***Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.***

De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través de un ciclo de mejora continua, la protección de los datos personales que resguarda el FOCIR.

A continuación, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad del FOCIR.

Para esta etapa, las unidades administrativas evaluaron y midieron los resultados de la implementación de las medidas de seguridad, verificado que las medidas realmente se estén aplicando y que funcionen para la correcta gestión del riesgo.

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

Para ello, se deberá observar si existen nuevos tratamientos de datos personales, nuevas amenazas, vulnerabilidades, y si las medidas de seguridad son acordes y suficientes para el nivel de riesgo asociado a cada uno de ellos. Es importante mencionar que esta actividad es constante, somo una acción de mejora continua, por lo que las unidades administrativas podrán identificar cambios en la evaluación de los riesgos.

Para los tratamientos de datos personales del FOCIR, se consideran los siguientes:

Revisión de cumplimiento de las políticas internas del FOCIR. Objetivo: asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la LGPDPPSO, los Lineamientos Generales, y demás normatividad que resulte aplicable.

Para ello, cuando se identifica algún cambio, se deberán realizar las siguientes actividades:

a) Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.
b) Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.
c) Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.
d) Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

Revisión del riesgo. Objetivo: identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, se implementarán los siguientes monitoreos:

a) Monitoreo del entorno físico. Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con:
   (i) personal de vigilancia en los accesos al edificio del FOCIR,
   (ii) control de acceso del personal con tarjeta de proximidad,
   (iii) control de acceso a través de bitácoras para visitantes y personal del FOCIR que olvidó su credencial,
   (iv) control de asistencia a través de huella digital, y
   (v) circuito cerrado de cámaras de vigilancia.

b) Monitoreo del entorno electrónico. Para la detección continua de amenazas y vulnerabilidades, la DTI revisará herramientas automatizadas de monitoreo, así como bitácoras de los sistemas informáticos del FOCIRI.

c) Actualización del plan de trabajo. Derivado de los monitoreos se realizarán actualizaciones en el plan de trabajo en los casos que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios se pondrán a consideración del área que apoya en el análisis de riesgos, la DTI y el Comité de Transparencia.

Revisión de avances del plan de trabajo. A través de los mecanismos que determinen las unidades administrativas del FOCIR y el Comité de Transparencia, harán una revisión de los

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

avances en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo, para hacer los ajustes correspondientes al mismo.

Actualización tecnológica. Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará una actualización del análisis de riesgo, análisis de brecha y plan de trabajo, por parte de la Dirección de Tecnologías de la Información.

Vulneraciones a la seguridad de los datos personales. En caso de identificar un incidente de seguridad que involucre datos personales, las unidades administrativas y la Dirección de Tecnologías de la Información informaran al Comité de Transparencia para decidir sobre las acciones pertinentes para mitigar dicho incidente.

Mecanismos de supervisión o revisión

El FOCIR contará con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

Las auditorías podrán ser internas o externas no vinculantes, realizadas por el INAI; administrativas realizadas el propio Comité con el apoyo de la Unidad de Transparencia, si así se estima pertinente.

Programa General de Capacitación

Con relación al programa de capacitación, la fracción VIII del artículo 33 de la LGPDPPSO señala que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Por su parte, el artículo 64 de los Lineamientos Generales señala lo siguiente:

> ***Capacitación***
> ***Artículo 64. Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.***
>
> ***En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:***
>
> ***I. Los requerimientos y actualizaciones del sistema de gestión;***
> ***II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;***
> ***III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y***

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

A partir de lo anterior, y en seguimiento a los trabajos que año con año realiza el FOCIR, respecto a las capacitaciones en materia de transparencia, acceso a la información, datos personales y archivos, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el FOCIR diseñará y aplicará diferentes niveles de capacitación del personal.

Se identificará el nivel y tipo de capacitación necesaria para el personal, de acuerdo con las responsabilidades asignadas y tomando en cuenta su perfil, especialmente de aquéllos involucrados en el tratamiento de datos personales.

Asimismo, se debe evaluar la eficiencia y eficacia de la capacitación, a través de criterios de evaluación que determinen el nivel de competencia aceptado por el FOCIR, y mantener un registro por persona servidora pública.

Para la elaboración del Programa de Capacitación, el FOCIR tomará en cuenta lo siguiente:

a) Los requerimientos y actualizaciones del sistema de gestión;
b) La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;
c) Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
d) Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Por lo que, la Unidad de Transparencia deberá elaborar el Programa Anual de Capacitación en materia de Datos Personales, de acuerdo con el calendario que publica el INAI.

a) Corto Plazo 2024

Sensibilización del personal que integra el FOCIR. Para esta meta se prevé coordinar que el personal de nuevo ingreso realice el curso de Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos, con el objetivo de que les permita internalizar la importancia de la protección de datos personales, así como identificar hábitos que ponen en riesgo la protección de datos personales.

b) Mediano plazo 2024 y 2025

Formación en protección de datos personales. Para esta meta se coordinará que las personas servidoras públicas tomen cursos o talleres que permitan identificar los procedimientos a seguir en la atención de solicitudes de derechos ARCO, la actualización de avisos de privacidad e inventarios de tratamientos, para la revisión y actualización de medidas de seguridad, para reducir los riesgos de vulneración de datos personales.

c)Largo plazo 2024-2026

Fortalecimiento de la protección de datos personales. Para esta meta coordinará que las personas servidoras públicas tomen cursos que permitan consolidar al interior del FOCIR la protección de datos personales como una actividad intrínseca a sus funciones.

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

CURSO	PERSONAL ADSCRITO AL FOCIR QUE DEBERÁ REALIZAR LOS CURSOS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES	PLAZOS
Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados *Este curso aplica para todo el personal de nuevo ingresó*	Mandos Altos Mandos Medios Técnicos Operativos	Corto plazo durante 2024
Clasificación de la Información y Prueba de Daño / Clasificación de la Información	Mandos Altos Mandos Medios Técnicos Operativos	Mediano Plazo durante 2024 y 2025
Aviso de Privacidad del Sector Público	Mandos Medios Técnicos Operativos	Mediano Plazo, durante 2024 y 2025
Esquemas de Mejores Prácticas en Materia de Protección de Datos Personales en el Sector Público	Mandos Medios Técnicos Operativos	Mediano Plazo, durante 2024 y 2025
Fundamentos del Documento de Seguridad en Materia de Protección de Datos Personales	Enlaces de Transparencia de las Unidades Administrativas y Unidad de Transparencia	Mediano Plazo, durante 2024 y 2025
Elaboración del Documento de Seguridad en Materia de Protección de Datos Personales	Enlaces de Transparencia de las Unidades Administrativas y Unidad de Transparencia	Mediano Plazo, durante 2024 y 2025
Sistema de Gestión de Seguridad de Datos Personales Sector Público	Enlaces de Transparencia de las Unidades Administrativas y Unidad de Transparencia	Mediano Plazo, durante 2024 y 2025

El programa estará sujeto a la disponibilidad de cursos que publique el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

El Programa Anual de Capacitación en materia de Datos Personales deberá ser presentado a más tardar en la última sesión ordinaria de cada año del Comité de Transparencia, y deberá diseñarse de tal forma que permita el cumplimiento de las metas señaladas, así como de las necesidades específicas que se detecten durante su implementación.

Actualización del documento de Seguridad

El artículo 36 de la LGPDPPSO establece la obligación de la actualización del Documento de Seguridad cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En ese sentido, cuando se actualice alguno de los supuestos antes citados, las unidades administrativas informarán a la Unidad de Transparencia para que esta lo haga del conocimiento del Comité de Transparencia, con el objeto de que este determine si considera procedente la actualización del Documento de Seguridad.

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación

Todos los sistemas de tratamiento que integran el Documento de Seguridad del FOCIR deben mantenerse actualizados; sin embargo, se entenderá que las modificaciones implican la necesidad de actualizar el Documento de Seguridad cuando al adecuarse el nivel de riesgo reportado las medidas de seguridad resulten insuficientes, todo ello como resultado de la mejora continua.

VERSIÓN NÚMERO	FECHA DE PUBLICACIÓN	DESCRIPCIÓN DEL CAMBIO	MOTIVO
01	31 de mayo de 2024	Documento de nueva creación	Documento de nueva creación