Sección:	Unidad de Transparencia
Oficio:	UT-54/07/24
Asunto:	Respuesta a Solicitud de Información 320589124000006
Fecha:	10 de julio de 2024

KAMISAMA
Presente

Con el gusto de saludarlo (a), me permito dar respuesta a su atenta solicitud No. 320589124000006, recibida a través de la Plataforma Nacional de Transparencia.

EL documento de seguridad que ordena la ley general de datos personales publicada el 26 de enero de 2017.

Si no cuenta con el quiero una razon fundada de porque no se ha elaborado en 7 años y si dicen que tiene un avance quiero la documentación que lo compruebe.

Por lo anterior, adjunto al presente envio el Documento de Seguridad de este Instituto.

Esperando que la información sea de utilidad, me es precisa la ocasión para reiterarle mi respeto.

Atentamente

ESMERALDA MARTINEZ PUENTE
Jefa de la Unidad de Transparencia

C.c.p.- Mtra. Gizel Liliana Llamas Ibarra.- Directora General del IZEA.- Presente.
C.c.p.- Archivo.

INSTITUTO ZACATECANO DE EDUCACIÓN PARA ADULTOS

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

INTRODUCCIÓN

Se elabora el presente Documento de seguridad de conformidad de acuerdo a lo establecido en el artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO) se establece la obligación de elaborar un documento de seguridad.

OBJETIVO Elaborar un inventario de datos personales y de los sistemas de tratamiento. (Art. 33 f. III LGPDPSO)

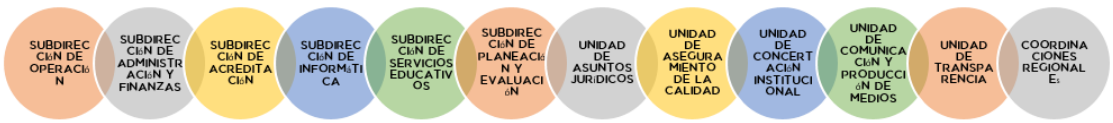
PARTE 1. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

DIRECCIÓN GENERAL

A. Dirección General del Instituto Zacatecano de Educación para Adultos

- Subdirección de Operación
- Subdirección de Administración y Finanzas
- Subdirección de Acreditación
- Subdirección de Planeación y Evaluación
- Subdirección de Servicios Educativos
- Subdirección de Informática
- Unidad de Asuntos Jurídicos
- Unidad de Aseguramiento de la Calidad
- Unidad de Concertación
- Unidad de Comunicación y Producción de Medios
- Unidad de Transparencia
- Coordinaciones Regionales

Nota: Existen Sistemas de Datos Personales (SDP) que aún y cuando son operados en las diferentes unidades administrativas ya sean del nivel central, regional o estatal, los responsables del manejo de los datos personales son principalmente la Subdirección de Administración y Finanzas por el manejo de la nómina y expedientes, así como los datos de proveedores, en el caso de la Subdirección de Acreditación le corresponde el resguardo de datos personales de los beneficiarios o usuarios de los servicios, en la Subdirección de Planeación y Evaluación los datos personales de proveedores, trabajadores, personas beneficiarias del subsistema, en la Subdirección de Servicios Educativos, datos personales de las personas a quienes se les realice capacitación y se tenga que llevar a cabo registro riguroso sobre todo en aquellos que tienen valor curricular, en la Subdirección de Informática por tratarse del área que solicita ante el INEA las cuentas de correo y contraseña y sirven de intermediarios para el control de los accesos a los sistemas SASA, RAF, SIGA, SINAPLAC, SIBIPLAC, que cuenta con la información de correos electrónicos a los cuales se cuenta con número de teléfono y también realiza el registro de los beneficiarios del subsistema, la Unidad de Asuntos Jurídicos en el que se tiene acceso a expedientes del personal y para efecto de investigaciones se tiene acceso a datos personales, la Unidad de Aseguramiento a la Calidad, quien por su actividad es verificar los domicilios y datos personales así como el acceso su información personal en sistema, la Unidad de Concertación en la firma de convenios, se accede a información de gerentes de empresas privadas mismas que son resguardadas y protegidas, la Unidad de Comunicación y Producción de Medios tienen protegidas las imágenes de personas a quienes una vez que se les da a conocer el aviso de privacidad se autoriza a publicar fotografías, la Unidad de Transparencia que tiene acceso a usuarios y contraseñas de los usuarios de la Plataforma Nacional de Transparencia y cuando se es requerida información puede tener acceso a expedientes de trabajadores cuya información está protegida y por último las Coordinaciones Regionales, que son quienes reciben y arman el expediente de los usuarios por lo tanto ellos tienen acceso a los documentos personales originales que ocupan para cotejar y tienen la obligación de digitalizarlos para completar el expediente en sistema.



Presentación

En enero de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), que tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados, siendo el Instituto Zacatecano de Educación para Adultos un sujeto obligado para cumplir con los deberes reconocidos por dicha ley.

A partir de ese momento, la Unidad de Trasparencia identificó la ruta que debería trazarse para encaminar el cumplimiento institucional en la materia, partiendo de la premisa de que el ámbito de trabajo se limitaría, en un principio, a la parte administrativa de este Instituto, y puso a consideración que el principal manejo de los datos personales se realizaba en algunas áreas específicas.

A partir del año 2022, se inició con la elaboración del Documento de Seguridad realizando una presentación ilustrativa la cual se compartió a todas las áreas del Instituto, a efecto emprender una cadena de acciones y trabajos que implicaron análisis, diseño, sensibilización, capacitación, retroalimentación, evaluación, recopilación y sistematización de información, datos y medidas de seguridad institucionales, con la participación de todas las áreas que reportaron tratamientos de datos personales. Como un primer instrumento en la materia y tomando en consideración que la propia Institución establece la necesidad de que las medidas de seguridad se encuentren debidamente documentadas, en particular, a través de la elaboración de un Documento de Seguridad (artículos 34 y 35), el 16 de enero de 2023, se concluyó con el primer Documento de Seguridad institucional el cual se integró:

I. Inventario de tratamientos de datos personales.
II. Análisis de riesgo.
III. Catálogo de medidas de seguridad.
IV. Análisis de brecha.

El Documento de Seguridad es un instrumento que permite a los sujetos obligados conocer el estado de cosas, las áreas de oportunidad y las líneas de acción para subsanar y atender los riesgos identificados en materia de seguridad de datos personales.

La Ley General establece la información básica que deberá contener dicho documento (artículo 35):

I. Inventario de datos personales y de los sistemas de tratamiento.
II. Funciones y obligaciones de las personas que tratan los datos personales.
III. Análisis de riesgo.
IV. Análisis de brecha.
V. Plan de trabajo.
VI. Mecanismos de monitoreo y revisión de las medidas de seguridad.
VII. Programa general de capacitación.

El propósito del Documento de Seguridad es que contuviera solo los elementos antes descritos fue presentar una primera radiografía institucional en materia de protección de los datos personales en su faceta administrativa, que reflejara las fortalezas, los pendientes y las áreas de oportunidad; y, constituyera un insumo para la toma de decisiones por parte de las instancias competentes en ese renglón para la implementación de acciones y medidas al respecto.

A partir de los hallazgos, en términos de los artículos 35, fracción V, y 84, fracciones IV y V, de la Ley General, se instruyó a la propia UT para que elaborara un plan de trabajo relacionado con el Documento de Seguridad.

Por ello, la UT perfiló el Plan de Trabajo en Materia de Protección de Datos Personales 2023 -2027 (Plan de Trabajo 2023 - 2027) como una herramienta complementaria y de instrumentalización del Documento de Seguridad, cuyos objetivos fundamentales fueron los siguientes:

1. Eliminar las brechas a través de la implementación de medidas de seguridad pendientes en cada uno de los tratamientos de datos personales identificados.

2. Consolidar y preservar los niveles de protección de los datos personales a través de mecanismos de monitoreo y revisión.

Este documento contempló la implementación de medidas de seguridad administrativas, técnicas y físicas. Es decir, entre el Documento de Seguridad y el Plan de Trabajo 2023 - 2027, así como los programas de capacitación que se aprobaron anualmente e integraron oferta en el rubro de datos personales, se contemplaron todos los elementos previstos en el artículo 35 de la Ley General, por lo que ambos constituyeron la base de la política institucional en materia de protección de datos personales.

El Plan de Trabajo 2023 - 2027 se previó ejecutar en un periodo de tres años y se implementó en dos etapas que se relacionaron con los propios objetivos:

I. Eliminar las brechas en las medidas de seguridad.
II. Implementar mecanismos de monitoreo

Por esa razón, en el segundo semestre de 2023, los insumos que componen el primer Documento de Seguridad debían actualizarse con la intención de entregar una radiografía actualizada en lo que respecta al Inventario de tratamientos de datos personales, el análisis de riesgos y el análisis de brecha, un nuevo plan de trabajo, mecanismos de monitoreo y revisión y capacitación a la luz de los hallazgos de los primeros años de trabajo en la materia.

Esto ha sido fundamental, por una parte, en tanto los tratamientos de datos personales se encuentran en constante evolución (creación, eliminación, fusión o actualización) y, por otra parte, porque se han implementado o sugerido todas las medidas de seguridad contempladas en el Plan de Trabajo 2023 - 2027, lo que se

reflejaría, cuando menos, en una brecha que se acerque al cien por 100% de cumplimiento.

Por las razones anteriores, en estas líneas se presenta el Documento de Seguridad–2023, cuyos insumos se alinean a lo dispuesto por el artículo 35 de la Ley General, los cuales se desarrollan más adelante en los apartados correspondientes:

I. Inventario de tratamientos de datos personales.
II. Listado de personas que intervienen en los tratamientos de datos personales.
III. Análisis de riesgo.
IV. Análisis de brecha.
V. Plan de trabajo 2024–2027.
VI. Mecanismos de monitoreo y revisión.
VII. Capacitación.

Los propósitos fundamentales de este Documento de Seguridad–2024 son:

I. Fortalecer la política institucional en la materia que ha sido implementada a lo largo de estos años.
II. Diseñar e implementar nuevas herramientas y medidas de seguridad que permitan profundizar en el cuidado de los datos personales. En términos del Plan de Trabajo que se describe más adelante, estos trabajos se circunscribirán al periodo de administración de la Directora General del IZEA Maestra Gizel Liliana Llamas Ibarra, por lo que, al concluir con los propósitos del presente documento, será necesario valorar su actualización.

I. Inventario de datos personales y de los sistemas de tratamiento

El Inventario de Tratamientos de Datos Personales (Inventario) es el control documentado que se lleva a cabo de los tratamientos de datos personales que realizan las áreas/órganos, contemplado en los artículos 33, fracción III y 35, fracción I, de la Ley General como un elemento del Documento de Seguridad.

La primera versión de dicho documento se realizó el primer semestre de 2023, en el que la UT trabajó con las áreas bajo la premisa de una coordinación interna para localizar todas las bases de datos personales de carácter administrativo en posesión de este Instituto.

El Inventario se actualiza permanentemente de conformidad con la información o los cambios que las propias áreas responsables solicitan a la UT en cada uno de los elementos de los tratamientos de datos personales o, en su caso, por su registro inicial, fusión o eliminación. A partir de 2022, se mantiene actualizado el Inventario de Datos Personales.

Los elementos que actualmente se identifican en el Inventario de cada uno de los tratamientos son los siguientes:

- Nombre de la unidad administrativa.
- Nombre del tratamiento.
- Finalidad.
- Fundamento normativo.
- Datos personales que se recaban.
- Forma de obtención de los datos personales.
- Cargos de las personas que tienen acceso a la base de datos.
- Tipo de soporte en el que se almacena la base de datos personales.
- Referencia documental conforme al Catálogo de Disposición Documental vigente.
- Información sobre transferencias de datos personales.
- Plazo de conservación.

El Inventario identifica, a través de una clave alfabética, cada una de las áreas responsables que tratan datos personales y con un número alfanumérico los

tratamientos bajo su responsabilidad (por ejemplo, área: A; tratamientos: A1 , A2, A3, así consecutivamente).

En un principio se contó con el registro de 12 áreas y/u órganos que tratan datos personales, con un total de 20 tratamientos registrados.

Este insumo ha implicado retroalimentación y acompañamiento permanente para orientar y sensibilizar al personal involucrado con los tratamientos de datos personales sobre las obligaciones en la materia.

La importancia de registrar la información exacta, además de cumplir con una obligación legal, radica en que las propias áreas puedan contar con esa información de manera permanente para ubicar e identificar los procesos que implican tratamiento de datos personales y el personal responsable de proteger, con un enfoque particular, el ciclo de vida de los datos personales que se tratan en las actividades cotidianas.

A partir de la integración del Inventario, se fueron elaborando los avisos de privacidad respectivos.

Los avisos simplificados fueron elaborados para que se colocaran en las instalaciones de cada una de las áreas responsables que así lo requirieran, en tanto se recaban datos de manera presencial; mientras que los integrales se ubicaron en el repositorio de avisos de privacidad integrales del Portal de Datos Personales, así mismo los avisos de privacidad que son publicados después de compartir alguna fotografía.

Los avisos se pueden consultar en el repositorio: https://izea.inea.gob.mx

Cabe señalar que los Avisos se actualizan constantemente por parte de las áreas u órganos, en tanto se modifican los tratamientos de datos personales o se registran nuevos que lo requieren.

La UT funciona como facilitadora de la publicación de los Avisos Integrales; por tanto, la implementación del aviso simplificado, así como la actualización de los avisos integrales, corren a cargo de las áreas u órganos responsables.

II. Listado de personas que intervienen en los tratamientos de datos personales

El Listado del Personal que Interviene en el Tratamiento de Datos Personales (Listado) es un elemento del Documento de Seguridad previsto en el artículo 35, fracción II de la Ley General.

En el 2022, la UT solicito a todas las áreas el listado para iniciar con la elaboración del inventario de seguridad y de ahí contar con los nombres de las personas que intervienen en el tratamiento de datos personales, en donde se había perfilado que, a lo largo del siguiente año, se materializaría una parte del referido plan, cuyo propósito inicial era la implementación de las medidas de seguridad recomendadas.

En ese sentido, como primera medida de seguridad de carácter administrativo prevista en el Plan de Trabajo 2023–2027, se les solicitó a todas las áreas que implementaran y resguardaran el Listado y remitieran a la UT una copia, para formar parte de las medidas de seguridad contempladas en el Plan de Trabajo. Se aclaró que debía elaborarse un listado por cada uno de los tratamientos registrados en el Inventario.

Para facilitar la implementación de dicha medida, la UT proporcionó guía práctica mediante correo electrónico a las áreas que les permitieran rescatar el listado correspondiente por cada uno de los tratamientos, los cuales fortalecieron para identificar el área de que se trata, el tratamiento respectivo, el número de personas que intervienen en él, su nombre, su cargo, la dirección de su oficina, la función que realiza sobre el tratamiento, el formato en que lo realiza y el fundamento normativo que lo faculta para realizarlo.

Como producto de esta medida, se integró el Listado que permite identificar el universo de personas servidoras públicas que intervienen en los tratamientos de datos personales y dimensionar la importancia de regular dicha actividad en el Instituto.

Posteriormente, como un mecanismo de monitoreo y revisión, se solicitó a las áreas la actualización de esta medida de seguridad cada semestre.

III. Análisis de Riesgo

Documento de Seguridad y ante la necesidad de determinar las medidas de seguridad que debían adoptar las áreas responsables, resultaba necesario conocer el nivel de riesgo que representaba cada tratamiento de datos personales (artículos 32, fracción I, 33, fracción IV y 35, fracción III de la Ley General).

Para ello, fue necesario calcular los factores de riesgo por tipo de dato, por tipo de acceso y por entorno desde el cual se realizan los tratamientos de los datos personales.

En el cálculo del nivel de riesgo de cada uno de los tratamientos registrados se usó como referencia la Metodología de Análisis de Riesgo, la cual se conoce así por las tres variables en las que se enfoca para determinar el nivel de riesgo de los datos personales:

A. Beneficio para el afectante.
B. Accesibilidad para el afectante.
C. Anonimidad del afectante. La metodología específica que se usó para el análisis de riesgo en este Instituto

Una vez que se calculó el nivel de riesgo latente por cada tratamiento de datos personales, fue posible diseñar estrategias para identificar los modelos de medidas de seguridad que debían aplicarse a cada uno de ellos y se integraron al primer Documento de Seguridad.

A partir del Plan de Trabajo 2023–2027, particularmente las Directrices para la Implementación de Mecanismos de Monitoreo y Revisión (Directrices), previstas para la segunda etapa de aquél, se contempló la actualización de este indicador como una de las acciones para la reformulación del Documento de Seguridad.

El primer análisis de riesgos del año 2023 se realizó sobre 30 tratamientos de datos personales registrados en ese momento, de 7 áreas u órganos de carácter administrativo, cuya cantidad de tratamientos ilustrada en porcentajes por nivel de riesgo fueron los siguientes:

Por su parte, la actualización de enero de 2023 se realizó sobre 34 tratamientos de datos personales registrados, de 12 áreas u órganos administrativos, cuya cantidad de tratamientos ilustrada en porcentajes por nivel de riesgo fueron los siguientes:

IV. Análisis de Brecha

El análisis de brecha permite identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados. Por ejemplo, si se recomienda implementar al tratamiento un conjunto de medidas y el área responsable informa que hacen falta implementar algunas, la identificación de lo que hace falta se conoce como brecha. Para tener una referencia institucional, el primer Catálogo de Medidas de Seguridad (Catálogo) se construyó a partir de los parámetros normativos y buenas prácticas que se desprenden de la propia Ley General, las políticas institucionales de seguridad de la Institución y la asesoría de la Subdirección de Informática.

En este documento se describen las medidas de seguridad administrativas, físicas y técnicas –complementarias a las políticas de seguridad generales de la Institución.

Posteriormente, a partir de la implementación del Plan de Trabajo 2023–2027, particularmente las Directrices previstas para la segunda etapa de aquél, se contempló la actualización de este indicador como una de las acciones para reformular el Documento de Seguridad.

Una vez que se obtuvieron los niveles de brecha de los tratamientos registrados por las áreas y los órganos conforme a las respuestas que fueron registradas por las personas responsables y la aplicación de la metodología diseñada para ello, se compartió la base de datos completa que registra toda la información que se reportó por las áreas y órganos en el análisis de brecha conforme al formulario puesto a disposición.

V. Plan de trabajo en materia de protección de datos personales

El Plan de Trabajo 2023–2027, toma como referencia las acciones realizadas en el marco del plan que le precedió, a propósito del cual se consolidaron medidas de seguridad de datos personales y se gestaron mecanismos iniciales de monitoreo y revisión.

Debido a que se obtuvieron resultados óptimos en la primera etapa de la implementación de las obligaciones y se tiene certeza de las áreas de oportunidad y de crecimiento, el Plan de Trabajo 2023–2027 tiene dos propósitos fundamentales:

1. Robustecer y fortalecer las medidas de seguridad implementadas, a través de herramientas y estrategias que ayuden a profundizar en el cuidado de los datos personales.

2. Diseñar nuevas acciones y medidas de seguridad especializadas para el cumplimiento de principios y deberes en la materia.

A partir de dichos objetivos, a continuación, se desarrollan las actividades que conformarán el Plan de Trabajo 2023–2027 (artículo 35, fracción V de la Ley General), en el que se contempla un trabajo de cuatro años, tomando en consideración que se complementa con los Mecanismos de Monitoreo y Revisión y el rubro de Capacitación.

OBJETIVO 1.

Fortalecimiento de las medidas de seguridad diseñadas

Sistema de Gestión para la Protección de Datos Personales Desde la publicación de la Ley General, la implementación de cada una de las disposiciones y obligaciones legales ha significado un reto para este Instituto y, particularmente, para las personas involucradas en el tema, en la medida que representó procesos y conceptos novedosos.

Por otro lado, destaca la disposición legal que refiere a que las acciones relacionadas con las medidas de seguridad para el tratamiento de datos personales deberán estar documentadas y contenidas en un sistema de gestión.

La Ley General refiere como sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales (artículo 34). Es decir, es el nodo que debe contener todo lo referente a la política institucional en el rubro.

En una primera instancia, el Portal de Datos Personales se gestó como el cigoto de un sistema de gestión que permitiera convertirse en un espacio de consulta permanente para titulares de datos personales, personas servidoras públicas involucradas en el tema y público en general. Sin embargo, no resultaba suficiente para automatizar procesos y transitar hacia la autogestión de medidas de seguridad.

El Instituto pretende consolidar el nivel de protección de los datos personales y materializar, de manera innovadora y bajo un esquema de mejores prácticas, el sistema de gestión a que refiere el artículo 34 Ley General.

La razón del desarrollo bajo esta funcionalidad es la accesibilidad de las personas usuarias, pues evita descargar y/o instalar aplicaciones. Con acceso a internet es suficiente para ingresar a dicho sistema.

Actualmente se trabaja en un esquema de colaboración cuya intervención técnica coadyuvará a la culminación de las últimas etapas del desarrollo, así como su instalación y puesta en marcha.

La síntesis y minimización de los procesos internos para la implementación y cumplimiento de cada uno de los principios y deberes previstos en la Ley General, lo que redundará en ahorro de tiempo y de recursos (humanos y materiales).

Asimismo, las personas responsables de las áreas y los órganos que tratan datos personales podrán verificar, consultar y actualizar la información en torno a los tratamientos bajo su responsabilidad.

Todo lo anterior trascenderá efectivamente en el nivel de protección de los datos personales, el cumplimiento en la materia y el ahorro de tiempo en las gestiones administrativas con esos propósitos.

La previsión para la conclusión del desarrollo del Documento de Seguridad y puesta en marcha, en su primera etapa, es durante el primer semestre del 2023.

Atención de las brechas existentes

Como resultado del Análisis de Brecha que se presenta en este Documento de Seguridad–2023, se advirtieron aquellos tratamientos cuyas medidas de seguridad (administrativas, físicas o técnicas) se reportaron como no implementadas o se encuentran en vías de implementarse.

Para la consecución del objetivo en el que se circunscribe la presente acción, es indispensable que todos los tratamientos de datos personales tengan un cumplimiento de 100% de medidas de seguridad implementadas.

Por lo anterior, en el segundo semestre de 2023 se diseñará un esquema de trabajo con aquellas áreas identificadas en el caso que se describe para su atención prioritaria, mismo que será implementado y desahogado a lo largo del año citado.

Acompañamiento de proyectos institucionales

Uno de los hallazgos más relevantes en la primera fase de la implementación de las obligaciones en la materia, fue que los proyectos institucionales que impliquen tratamiento de datos personales debían contemplar la perspectiva de protección de datos personales desde su planeación.

El cumplimiento de los principios como el de finalidad, licitud, consentimiento, proporcionalidad, legitimidad, se dará en la medida en que se analice la compatibilidad del proyecto o actividad con estos principios, se tomen las medidas pertinentes para adecuarlos a los mismos y se tenga consciencia del deber de cuidado de los datos personales en todo su ciclo de vida.

Por la relevancia de crear un insumo claro y didáctico que permita a las áreas conocer de antemano la política de protección de datos personales y su relevancia para los proyectos que se emprendan, se propone elaborar unas Directrices para Integrar la Perspectiva de Protección de Datos Personales en los Proyectos Institucionales.

Este documento se planea diseñar y difundir en el segundo semestre de 2024.

Esto implicará también generar un esquema de acompañamiento permanente a todas las áreas para la atención oportuna de proyectos o actividades de nueva creación que impliquen tratamiento de datos personales.

Identificación del ciclo de vida de los datos personales

El ciclo de vida de los datos personales permite conocer las fases por las que pasa la información desde su obtención hasta su destrucción, independiente del formato en el que se almacenen los datos personales.

Si bien, el Inventario identifica los elementos necesarios que muestran la naturaleza y alcance de los mismos, no proporciona un panorama real y actualizado del ciclo de vida a que son sometidos los datos personales en cada uno de ellos.

Por tanto, un diagrama que refleje el ciclo de vida de los datos personales por cada uno de los tratamientos registrados permitirá complementar el Inventario, identificar riesgos a que pueden estar sujetos los datos personales, los diferentes tratamientos que recibe la información, su tipo de almacenamiento, el periodo de conservación, así como verificar el cumplimiento de principios y deberes, entre otras cosas.

Esta acción robustece las medidas de seguridad implementadas y se planea materializar a lo largo del año 2024, en la medida que implica la elaboración, hasta el momento, del ciclo de vida de los datos personales (número de tratamientos registrados actual) y que pudiera significar, inclusive, modificación de manuales de procesos.

Actualización y seguimiento de medidas de seguridad

Uno de los objetivos del Plan de Trabajo 2023–2027 fue preservar el nivel de cumplimiento y protección conseguido en la primera etapa a través de la implementación de mecanismos de monitoreo y revisión de las medidas de seguridad, además de la mejora de los procesos en el tratamiento de los datos personales y el acompañamiento para la ejecución de todas las medidas de seguridad.

Por lo anterior, se formularon las mencionadas Directrices como un primer acercamiento que orientara el diseño y la implementación de los mecanismos para fortalecer el cumplimiento de las medidas de seguridad en los tratamientos de datos personales (contemplando su nivel de riesgo), a partir de los cuales fuera posible

integrar a todas las áreas/órganos que tratan datos personales, generar un diálogo sobre el estado de cosas y detonar acciones en función del resultado de los monitoreos.

En ellas se consideró que los mecanismos de monitoreo y revisión debían tener estos propósitos:

Actualizar los insumos y las medidas de seguridad que así lo requieran. Reforzar las recomendaciones que se realizaron a través de las medidas de seguridad implementadas en la primera etapa del Plan de Trabajo 2023–2027.

Establecer un espacio de trabajo en el que se resuelvan dudas e inquietudes sobre el tema, se identifiquen posibles amenazas o vulneraciones y se robustezca la cultura de la protección de datos personales en la institución.

Derivado de los resultados obtenidos, es necesario continuar con la implementación de dichos mecanismos de monitoreo, especialmente el que se refiere a la actualización de indicadores y medidas de seguridad, en tanto existen algunas que deben realizarse periódicamente para mantenerlas vigentes y actualizadas.

Estas actualizaciones se calendarizarán semestralmente.

Mesa de atención

Una de las necesidades que se advirtieron tras la implementación del Plan de Trabajo 2023 –2027, es la de brindar atención oportuna a todo el personal que interviene en el tratamiento de datos personales, para resolver dudas, preguntas, orientar sobre trámites, acciones o insumos relacionados con la materia y conducir a buen puerto sus inquietudes de manera cotidiana, a través de canales de comunicación accesibles e identificables.

Esto es relevante en la medida en que algunas dudas o preguntas pudieran implicar posibles vulneraciones a datos personales, modificaciones a los instrumentos registrados, actualizaciones a los avisos de privacidad, entre otras cosas.

En principio, se preverá que este mecanismo de comunicación sea a través correo electrónico.

Esta medida requerirá de personas especializadas en el tema para brindar la atención y promover este mecanismo de comunicación a través de la RED que más adelante se propone.

OBJETIVO 2. Nuevas acciones y medidas de seguridad especializadas

Primera acción

Actualización del Catálogo de Medidas de Seguridad

La finalidad de las medidas de seguridad enfocadas especialmente en la protección de los da tos personales es evitar cualquier daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado en las actividades cotidianas de las áreas/órganos que integran el Instituto y que pudieran afectar su confidencialidad, dejando en estado de vulnerabilidad a sus titulares.

El primer esquema de seguridad fue implementado a partir del Catálogo confeccionado con medidas de seguridad irreductibles que ahora deberán convertirse en básicas.

De esta forma y en la medida que el Catálogo ha sido cumplido e implementado para la mayoría de los tratamientos de datos personales y que, a través del primer objetivo planteado en este documento se garantizará que se mantenga un cumplimiento óptimo, resulta relevante para la institución el diseño y elaboración de nuevas medidas de seguridad especializadas en la protección de datos personales, que respondan a necesidades particulares, con la colaboración de áreas especializadas en tecnologías, seguridad, archivos, entre otras. Por tanto, esta acción se planea elaborar e implementar a partir del primer semestre de 2025, con la finalidad de perfilar un nuevo plan de trabajo en la materia conforme a estas nuevas medidas de seguridad.

Segunda acción

Red de personas responsables y coordinadoras

En el marco del Plan de Trabajo 2023–2027, como una medida de seguridad administrativa, se planteó que cada área u órgano que tratara datos personales designara una persona responsable de seguridad de datos personales para coordinar y auxiliar en la implementación de las medidas de seguridad establecidas, con el fin de que se preserven y exista una comunicación directa con el Instituto.

En esa tesitura, se conformó el Directorio de responsables de seguridad de datos personales del Instituto, a cargo del tema en las áreas administrativas/órganos que cuentan con tratamientos de datos personales.

Cabe resaltar que son las áreas las que nombran o sustituyen a las personas responsables.

No obstante, desde una perspectiva más exigente, este esquema no resulta suficiente en el momento en que se busca masificar y profundizar el conocimiento en todas las personas que intervienen en los tratamientos de datos personales.

Factores como que las personas designadas como responsables cumplen varias funciones al interior de su área y el tema de protección de datos personales no se atiende de manera exclusiva, aunado a que los tratamientos de datos implican ciertas particularidades que solo conocen quienes se inmiscuyen cotidianamente, obstaculizarían alcanzar este nivel de profundidad. Por tanto, se propone una nueva estrategia de comunicación con las áreas responsables para permear en toda la institución y fortalecer el nivel de conocimiento en todas las personas servidoras públicas.

Esta estrategia implicaría:

- Mantener la figura de responsable de seguridad en datos personales por área u órgano.
- Designar una persona representante/coordinara por cada tratamiento de datos personales.
- Abrir mecanismos de comunicación por parte del Instituto de fácil acceso (correo electrónico, chat, etc.) disponible a todo el personal para que resuelvan dudas de manera puntual y rápida.

Esta acción, en la medida que resulta relevante implementar las demás acciones y mecanismos de monitoreo a través de la nueva RED, se planea consolidar en el segundo semestre de 2023.

Tercera acción

Divulgación de la información

Considerando que una acción fundamental para consolidar la cultura de la protección de datos personales es la difusión de insumos e información relativa al tema, y tomando en cuenta los resultados que se obtuvieron a través de la difusión de infografías periódicas a todas las personas servidoras públicas de este Instituto, se propone en este nuevo Plan de Trabajo 2023–2027 la divulgación del conocimiento e información en la materia más robusta.

Para ello, se fortalecerá la colaboración con la Dirección General de Comunicación Social a raíz del proyecto de divulgación de infografías que se emprendió en el marco del primer plan de trabajo, con el objetivo de encontrar alternativas complementarias de difusión del conocimiento y la información, que pudiera resultar de interés para la institución y público en general a través de insumos y/o productos audiovisuales.

El alcance del nuevo esquema colaborativo será diseñado en conjunto con las áreas involucradas y a través de un esquema de trabajo en particular.

Cuarta acción

Conservación y borrado seguro de información electrónica

Debemos considerar el periodo de conservación y los procedimientos de transferencias primaria (al archivo de concentración) y secundaria (al archivo histórico), así como de baja documental de expedientes administrativos.

De esta manera, se identificaran los plazos y procedimientos para la conservación y eliminación de los datos personales que se resguarden en documentos o bases de datos conforme a su serie documental, independientemente del formato en que se almacenen.

Actualmente, los tratamientos de datos personales se realizan, en su mayoría, en formato electrónico.

Además, se advirtió que la conservación de este tipo de archivos se realizaba más tiempo del permitido.

Por tanto, resulta necesario diseñar e implementar una estrategia para la conservación adecuada de archivo electrónico y, especialmente, de su borrado seguro, una vez que la información ha cumplido con su plazo de conservación, de conformidad con los instrumentos de archivo.

Esta estrategia deberá ser diseñada en conjunto con la Coordinación de Archivos, para contar con un procedimiento que dé certeza sobre el ciclo de vida de los datos personales en formato electrónico.

Por tanto, se propone que en 2024 se establezca un grupo de trabajo en conjunto con ambas áreas, hasta en tanto se tenga certeza de los alcances del Documento de Seguridad en la institución, para acordar un procedimiento a implementarse en los años subsecuentes.

Quinta acción

Atención de solicitudes ARCO

Resulta importante que las áreas y/u órganos cuenten con directrices claras para conocer la implicación de los derechos ARCO y cómo encausar y atender debidamente una solicitud de esta naturaleza a través de la UT, promoviendo que las personas titulares ejerzan sus derechos cuando lo estimen necesario.

De esta manera, se planea diseñar y difundir en el año de 2025 una Guía para la atención de solicitudes ARCO de uso interno para clarificar los alcances del ejercicio de estos derechos y establecer un procedimiento para encausar estas solicitudes de manera correcta y oportuna.

VI. Mecanismos de monitoreo y revisión

Los Mecanismos de Monitoreo y Revisión (Mecanismos) tienen como objetivo fundamental preservar el nivel de cumplimiento y protección conseguido en la implementación de las medidas de seguridad, además de la mejora de los procesos en el tratamiento de los datos personales (artículo 35, fracción VI de la Ley General).

Al respecto, la Ley General menciona que, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales (artículo 33, fracción VII). Por lo anterior, se proponen diversas acciones relacionadas con el monitoreo y la revisión del cumplimiento de los principios y deberes en materia de protección de datos personales, que a continuación se desarrollan.

VII. Capacitación en datos personales

Desde la implementación de la primera etapa del Plan de Trabajo 2019–2022, se ha incorporado una oferta de capacitación especializada al personal involucrado en el tratamiento de los datos personales a través de los Programas anuales de capacitación en materia de transparencia, acceso a la información y protección de datos personales

La capacitación debe retomarse en este nuevo Plan de Trabajo 2023–2027 con una perspectiva de mayor alcance, pues la que se ofreció en la primera etapa, principalmente, estuvo dirigida a las personas designadas como responsables de seguridad de datos personales, cuya premisa ha sido la difusión del conocimiento al interior de sus áreas, además de la puesta a disposición de todos los materiales de capacitación e información en el Portal de Datos Personales para su consulta permanente.

Sin embargo, cada tratamiento de datos personales representa retos diferentes para la confidencialidad de la información. Por ello, las personas que tratan cotidianamente los datos personales deben tener presente las recomendaciones en la materia y es necesaria una nueva planificación de capacitación que sea masiva, especializada para cada área u órgano, que se refleje en insumos específicos para atender problemáticas puntuales, que evalúe el nivel de conocimiento y que aproveche las herramientas tecnológicas.

Por lo anterior, anualmente y a través de los Programas de Capacitación respectivos, se ofertarán capacitaciones especializadas en el tema que cubran esas expectativas, cuyos contenidos podrán ser consultados una vez que sean aprobados por el Comité de Transparencia.

Inicialmente y para el año 2023, el Programas de Capacitación prevé las siguientes líneas vinculadas con protección de datos personales:

Continuidad en lo que toca a la homologación de los conocimientos básicos de las personas designadas como enlaces de transparencia, a través de diversos cursos albergados en el CEVINAI, entre ellos, "Introducción Ley General Protección Datos Personales Posesión Sujetos Obligados".

Diseño, planeación e impartición de un curso mejores prácticas de protección de datos, dirigido a las personas designadas como responsables de seguridad de datos personales y/o al personal que interviene en los tratamientos de datos personales. Diseño, planeación e impartición de un curso especializado en materia de protección de datos personales, en coordinación con áreas especializadas en temas de seguridad de información, dirigido a las personas designadas como responsables de seguridad de datos personales y coordinadores de tratamientos de datos personales.

Continuidad a la impartición de cursos de inducción para personas de nuevo ingreso o reingreso al Instituto que incluye, entre otros, el tema de datos personales.

VIII. Consideraciones finales

Tomando en consideración las acciones planteadas y el hecho de que se trata de una proyección de largo alcance que supone la posibilidad de que se presenten coyunturas imprevistas y ello impacte en los tiempos de cumplimiento, resulta de gran relevancia para la institución la existencia de un área encargada de la implementación de las obligaciones legales en materia de protección de datos personales y la posibilidad de contar con un Oficial de Protección de Datos Personales en términos de la Ley General, para atender debidamente las necesidades de cada una de las áreas y se eleve el nivel de protección de los datos personales.