Querétaro; Qro. 3 de abril de 2023.

DOCUMENTO DE SEGURIDAD

DEL CENTRO DE CONCILIACIÓN LABORAL DEL ESTADO DE QUERETARO

Presentación

El presente Documento de Seguridad se elabora en cumplimiento a las obligaciones establecidas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales en Protección de Datos Personales para el Sector Público, que establecen que los responsables del tratamiento de datos personales deberán establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Al respecto, entre las acciones que deberá realizar este Centro de Conciliación Laboral del Estado de Querétaro, responsable del tratamiento de datos personales para cumplir con el deber de seguridad, se encuentra la elaboración de presente instrumento, como el medio que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por este sujeto obligado para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Este documento, estructura la información remitida por las áreas responsables que manifestaron dar tratamiento a datos personales, relacionado con su uso, registro, organización, conservación, elaboración utilización comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia, disposición o cualquier otra operación aplicable a ellos.

Por lo anterior, cuenta con los apartados siguientes:

✓ El inventario de datos personales y de los sistemas de tratamiento;

✓ Las funciones y obligaciones de las personas que traten datos personales;

✓ El análisis de riesgos;

✓ El análisis de brecha;

✓ El plan de trabajo;

✓ Los mecanismos de monitoreo y revisión de las medidas de seguridad, y

✓ El programa general de capacitación.

En ese sentido, en cumplimiento de las obligaciones antes descritas, a continuación, se presenta el documento de seguridad del Centro de Conciliación Laboral del Estado de Querétaro con los elementos informativos que establece el artículo 35 de la Ley General.

Glosario

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los datos personales, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.

Bases de datos: Conjunto ordenado de datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Centro: Centro de Conciliación Laboral del Estado de Querétaro.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran

sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Documento de Seguridad: Instrumento que describe y da cuenta, de manera general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Evaluación de impacto en la protección de datos personales: Evaluación mediante la cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

Instituto o INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Criterios de Evaluación: 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.

Ley General o LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Ley Orgánica o LOCCLEQ: Ley Orgánica del Centro de Conciliación Laboral del Estado de Querétaro.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Portabilidad de datos personales: Prerrogativa del titular de obtener una copia de los datos que ha proporcionado al responsable del tratamiento en un formato estructurado que le permita seguir utilizándolos.

Reglas o Reglas de Operación: Reglas de Integración y Funcionamiento de la Unidad de Transparencia y del Comité de Transparencia del Centro de Conciliación Laboral del Estado de Querétaro.

Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

Responsable: Sujeto obligado de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que decide sobre el tratamiento de los datos personales.

Revisión: Actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en este Programa.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Titular: Persona física a quien corresponden los datos personales.

Transferencias: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Unidad Administrativa o área: Área del Centro de Conciliación Laboral del Estado de Querétaro a la que se le confieren atribuciones específicas en la Ley Orgánica del Centro de Conciliación Laboral, equivalente que sea superior a un manual de organización.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley de Transparencia y Acceso a la Información Pública.

Elementos del Documento de Seguridad

Como fue referido previamente, el documento de seguridad se define como un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales con que cuenta el Centro de Conciliación Laboral.

Para ello, el artículo 35 de la Ley General establece los elementos mínimos que el documento de seguridad debe contener, siendo estos:

1. Inventario de datos;

2. Funciones y obligaciones de las personas que tratan datos;

3. Análisis de riesgos;

4. Análisis de brecha;

5. Plan de trabajo;

6. Mecanismos de revisión y monitoreo de las medidas de seguridad y,

7. Programa general de capacitación.

En ese sentido, en las páginas siguientes, se abordará cada uno de los elementos que debe contener el documento de seguridad, con base en lo establecido en la mencionada Ley y, como complemento, en lo dispuesto por los Lineamientos Generales y los documentos de apoyo publicados por el INAI.

I. Inventario de datos personales

De acuerdo con lo establecido en los artículos 33, fracción III y 35, fracción I de la LGPDPPSO y 35 de los Lineamientos Generales, los sujetos obligados deben elaborar un inventario de datos personales con la información básica de cada tratamiento de datos personales, en el cual deban considerarse entre otros elementos, los siguientes:

• Catálogo de medios físicos y/o electrónicos a través de los cuales se recaban los datos;

• Las finalidades para las cuales son recabados y tratados los datos personales;

• El catálogo de tipo de datos tratados, y

• El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales.

En ese sentido, son 2 las áreas responsables del Centro de Conciliación Laboral que manifestaron dar tratamiento a datos personales por lo que se integró un inventario, con el apoyo y orientación de la Unidad de Transparencia, mismo que se acompaña al presente como Anexo 1 y en el cual se señalan los tratamientos que actualmente se realizan siendo coincidentes con los avisos de privacidad elaborados y publicados en la página electrónica del Centro, en el apartado de Protección de Datos, subapartado “Avisos de Privacidad”.

Las distintas secciones del inventario de tratamientos de datos personales del Centro se conforman de la siguiente manera:

Medios de obtención de los datos personales	Manera en la que los sujetos responsables obtienen los datos personales de los titulares. Puede ser de manera directa o indirecta.
Finalidades del Tratamiento de datos personales	Motivos por los que el sujeto responsable solicita los datos personales. Las finalidades deben de ser concretas, lícitas, explicitas y legítimas.
Datos personales que se obtienen para el tratamiento	Datos personales necesarios para que el sujeto obligado pueda dar atención al tratamiento. Se diferencian entre sensibles y no sensibles.
Medios de almacenamiento	Medio en el que se almacenan los datos personales, puede ser en formato físico, electrónico o ambos.
Servidores públicos con acceso al tratamiento	Personas de los sujetos responsables que, conforme al ámbito de sus atribuciones, tratan los datos personales.

Transferencia	Los datos personales que, en su caso, pueden estar sujetos a una comunicación dentro o fuera del territorio mexicano realizada a persona

Como resultado de dicho inventario, se desprendió que el Centro realiza un tratamiento de datos, principalmente de tipo identificativo y laboral, respecto del personal que en el labora o presta sus servicios, así como de quienes sustancian procedimientos de conciliación que deberán agotar los trabajadores y patrones, en asuntos individuales, conforme lo establecido por los párrafos segundo y tercero de la fracción XX del artículo 123, Apartado A, de la Constitución Política de los Estados Unidos Mexicanos y 684-A a 684- E de la Ley Federal del Trabajo.

Este insumo permite el análisis, desarrollo y concreción de medidas para el adecuado tratamiento de datos personales al interior de este sujeto obligado, con el ánimo de sensibilizar a las y los servidores públicos en la importancia de garantizar las acciones a través de las cuales se posibilite el efectivo ejercicio de la autodeterminación informativa, acorde con las medidas de seguridad referidas en líneas posteriores.

El inventario de datos personales reporta los tratamientos de las siguientes áreas:

Áreas administrativas	Tratamientos realizados
Sub dirección de Conciliación	Procedimiento de Conciliación Individual
Sub dirección Administrativa	Trámites de Recursos Humanos del Centro, Recursos Materiales y Servicios Generales Procedimientos de reclutamiento, selección de personal

II. Funciones y obligaciones de las personas que tratan datos personales.

Uno de los objetivos que se busca con este documento, es permear en las y los servidores públicos de este Centro, la importancia que tiene el adecuado tratamiento de los datos personales y, con ello, sensibilizarlos para garantizar la efectiva protección de la información personal que manejen, conforme al ámbito de sus atribuciones.

Bajo ese contexto, es necesario disponer de funciones y obligaciones las cuales deben ser observadas en todo momento por quienes intervengan de cualquier modo en el tratamiento de los datos personales recabados, mismos que para efectos del presente, se refieren a continuación:

• **Unidad de Transparencia**: Instancia a la que hace referencia el artículo 45 de la Ley General.

• **Enlace:** La persona designada por cada uno de los titulares de las áreas que integran al Centro responsable para la administración y custodia de los datos personales recabados.

• **Usuario**: La persona que, por sus actividades laborales y atribuciones legales, tenga acceso a los datos personales.

Para tal efecto, las funciones y obligaciones mínimas que deberán atender quienes conforme a sus atribuciones realicen el tratamiento de datos personales en cada sujeto responsable, son las siguientes:

Tipo	Funciones	Obligaciones
Unidad de Transparencia	1. Comunicar al personal del sujeto responsable el contenido del documento de seguridad.	1. Coordinar la implementación de medidas de seguridad para el tratamiento de datos.
	2. Observar los principios y deberes establecidos en la Ley General y los Lineamientos Generales para el adecuado tratamiento de los datos.	2. Verificar que los accesos a los sistemas de información garanticen niveles de seguridad adecuados.
	3. Incentivar la capacitación del personal.	3. Comunicar al responsable designado conforme al art. 85 de la LGDPPSO las vulneraciones de datos que se hayan suscitado.
	4. Establecer canales de comunicación con la Unidad de Transparencia, a fin de obtener asesoría u orientación	4. Autorizar la realización de copias de respaldo y/o recuperación de los datos personales.

	sobre el tratamiento de datos personales que realiza.	
		5. Informar, por lo menos una vez al año, al responsable designado conforme al art. 85 de la LGDPPSO respecto de nuevos tratamientos de datos o de la actualización de medidas de seguridad implementadas.

Tipo	Funciones	Obligaciones
Enlace	1. Observar los principios y deberes establecidos en la Ley de la materia para el adecuado tratamiento de los datos.	1. Supervisar la implementación de medidas de seguridad para el tratamiento de datos.
	2. Velar por que se realice un adecuado tratamiento de los datos personales, conforme a los principios y deberes establecidos en la Ley.	2. Llevar una bitácora de los accesos a los datos personales con que cuentan.
	3. Fungir como enlace con la Unidad de Transparencia.	3. Informar al responsable de las vulneraciones suscitadas.
	4. Proponer al responsable, la implementación y o actualización de medidas de seguridad, así como el desarrollo o adopción de esquemas de mejores prácticas, conforme a las disposiciones legales aplicables.	4. Elaborar el informe que el responsable debe remitir al responsable designado conforme al art. 85 de la LGDPPSO.
		5. Remitir a la Unidad de Transparencia el inventario de tratamiento de datos personales,

		cuando esta lo solicite, se realice un nuevo tratamiento de datos o se actualicen las medidas de seguridad.
		6. Mantenerse actualizado en los cursos, talleres o programas de capacitación relacionados con la materia.

Tipo	Funciones	Obligaciones
Usuario	1. Observar los principios y deberes establecidos en la ley de la materia para el adecuado tratamiento de los datos.	1. Utilizar los datos personales a los que tenga acceso, únicamente para el desempeño de sus atribuciones.
	2. Conocer las implicaciones legales y administrativas que conlleva el tratamiento indebido o no autorizado de datos personales.	2. Guardar secreto y confidencialidad de los datos a los cuales tenga acceso.
	3. Proponer la implementación de medidas de seguridad o esquemas de mejores prácticas que, en su caso, estime necesarias.	3. Abstenerse de borrar, destruir, dañar, alterar, sustraer, modificar o divulgar cualquier información relacionada con datos personales, sin que tenga la debida autorización expresa para ello.
		4. Informar sobre cualquier anomalía, error, imprecisión o fallo que detecten en los datos a los cuales tengan acceso.

Es importante precisar que, los titulares de los sujetos responsables están obligados a generar las acciones que estimen pertinentes para contar con el aviso de privacidad respectivo, previo al inicio del tratamiento de datos personales, a fin de dar cumplimiento al Principio de Información, establecido en los artículos 27 y 28 de la LGPDPPSO, así como 26 a 45 de los Lineamientos Generales.

Para tal efecto, la Unidad de Transparencia será la encargada de orientar y auxiliar a las áreas en el proceso de elaboración de sus avisos de privacidad, cuando así lo soliciten.

Estas funciones y obligaciones podrán ser modificadas por el Comité de Transparencia, a petición del responsable designado conforme al art. 85 de la LGDPPSO, salvaguardando en todo momento, el adecuado tratamiento de los datos personales al interior del Centro.

Las funciones y obligaciones de los involucrados en los tratamientos reportados en el Inventario de datos personales se documentan en el Anexo 2 que forma parte del presente.

III. Análisis de riesgos

Existen grandes retos a los que se enfrentan todas las instituciones, tanto públicas como privadas, uno de ellos es el prever y evitar lo inesperado, especialmente en un escenario que involucra las constantes y novedosas tecnologías de la información.

Por tal motivo, la Ley General establece la necesidad de contar con un análisis de los riesgos a los cuales se puede enfrentar el tratamiento de los datos personales durante su ciclo de vida; para muestra, en el documento denominado Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales, emitidas por el INAI, se indican los incidentes más comunes:

1. Robo de información en documentos y medios de almacenamiento desechados incorrectamente;

2. Empleados que acceden a datos personales sin la autorización correspondiente;

3. Empleados que revelan información a otras personas a través de engaños;

4. Robo o pérdida de equipos de cómputo, laptops, teléfonos inteligentes, tabletas, o memorias extraíbles con información personal, y

5. Acceso ilegal a las bases de datos personales por un externo.

Ante este escenario, resulta importante que los sujetos obligados, como lo es el Centro, realicen un análisis de riesgos, respecto de la información personal recabada, con el propósito de detectar las áreas de oportunidad y mejora necesarias para un adecuado tratamiento de esta.

Para tal efecto, en las subsecuentes líneas se aborda el análisis de riesgos, acorde con lo previsto en los artículos 33, fracción IV y 35, fracción III de la Ley General; y 60 de los Lineamientos Generales, con el propósito de considerar las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, en el cual se referirá lo siguiente:

III.1 Los requerimientos regulatorios, códigos de conducta o mejores prácticas.

Las Reglas de Integración y Funcionamiento de la Unidad de Transparencia y del Comité de Transparencia del Centro Conciliación Laboral disponen como uno de sus objetivos, la protección de los datos personales que obran en los archivos de las áreas.

Para ello, dicho ordenamiento prevé promover la capacitación de los servidores públicos del Centro, en el tema de protección de datos personales.

Por su parte, el Código de Ética de la Administración Pública Estatal establece como una de las Reglas de Integridad, la Información pública consistente en consolidar la

transparencia y rendición de cuentas en el servicio público, conforme al principio de máxima publicidad, el acceso a información pública que tenga bajo su cargo, tutelando en todo momento, los derechos de acceso, rectificación, oposición o cancelación de los datos personales, en los términos que fijen las normas correspondientes.

En esa tesitura, el Código de Ética de la Administración Pública Estatal indica que las y los servidores públicos sujetarán sus acciones, entre otros, a los principios constitucionales y legales de respeto a los derechos humanos, legalidad, honradez, lealtad, imparcialidad, eficiencia, eficacia y transparencia.

Cabe señalar que, tanto las Reglas de Integración y Funcionamiento de la Unidad de Transparencia y del Comité de Transparencia del Centro, como el Código de Ética de la Administración Pública Estatal, se encuentran publicados en la página electrónica del Centro https://www.cclqueretaro.gob.mx/index.php, en su apartado "Centro documental".

Como se aprecia, el Centro en su calidad de sujeto obligado y responsable del tratamiento de los datos personales que obran en sus archivos, se ha dado a la tarea de establecer disposiciones claras y precisas a las cuales deben sujetarse quienes en ella laboran.

III.2 El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida.

Para la elaboración del Documento de Seguridad fue de vital importancia identificar los tipos de datos personales, la sensibilidad de los mismos y el número de personas de quienes se tratan dichos datos para determinar el valor que representan para un atacante.

Los datos personales pueden clasificarse en cuatro categorías, de acuerdo con la criticidad de estos por nivel de riesgo inherente:

Datos con riesgo inherente bajo Esta categoría considera información general concerniente a una persona física identificada o identificable, que no corresponda a la información a la que refieren las otras tres categorías, como por ejemplo datos de identificación y contacto o información académica o laboral, tal como nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo y lugar de trabajo, idioma o lengua, escolaridad, cédula profesional, información migratoria, entre otra información que no refiera a las siguientes tres categorías.

Datos con riesgo inherente medio. Esta categoría contempla los datos que permiten conocer la ubicación física de la persona, tales como la dirección física, información relativa al tránsito de las personas dentro y fuera del país, y/o cualquier otro que permita volver identificable a una persona a través de los datos que proporcione alguien más. Por ejemplo: dependientes, beneficiarios, familiares, referencias laborales, referencias personales, etc. También son datos de riesgo inherente medio aquéllos que permitan inferir el patrimonio de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio,

ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados. Incluye el número de tarjeta bancaria de crédito y/o débito. Son considerados también, los datos de autenticación con información referente a los usuarios, contraseñas, información biométrica (huellas dactilares, iris, voz, entre otros), firma autógrafa y electrónica, fotografías, identificaciones oficiales, inclusive escaneadas o fotocopiadas y cualquier otro que permita autenticar a una persona. Dentro de esta categoría se toman en cuenta los datos jurídicos tales como antecedentes penales, amparos, demandas, contratos, litigios y cualquier otro tipo de información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

Datos con riesgo inherente alto. Esta categoría de datos contempla a los datos personales sensibles, que de acuerdo a la Ley incluyen datos de salud, los cuales se refieren a la información médica donde se documente el estado de salud física y mental, pasado, presente o futuro; información genética; origen racial o étnico, ideología, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual, hábitos sexuales y cualquier otro cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para el titular.

Datos con riesgo inherente reforzado. Los datos de mayor riesgo son los que de acuerdo con su naturaleza derivan en mayor beneficio para un atacante, por ejemplo:

Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o débito mencionado anteriormente en combinación con cualquier otro dato relacionado o 5 contenido en la misma, por ejemplo, fecha de vencimiento, códigos de seguridad, datos de banda magnética o número de identificación personal (PIN).

Las personas de alto riesgo son aquéllas cuya profesión, oficio o condición están expuestas a una mayor probabilidad de ser atacadas debido al beneficio económico o reputacional que sus datos personales pueden representar para un atacante. Por ejemplo, líderes políticos, religiosos, empresariales, de opinión y cualquier otra persona que sea considerada como personaje público. Asimismo, se considera a cualquier persona cuya profesión esté relacionada con la impartición de justicia y seguridad nacional. Tratar datos de personas de alto riesgo involucra que la base de datos contiene nombres de figuras públicas que pueden ser reconocidas a primera vista, así como información personal donde se infiera o se relacione

explícitamente con su profesión, puesto o cargo en combinación con datos de identificación como nombre, domicilio, entre otros. Es importante señalar que las categorías antes descritas se desarrollaron exclusivamente para la aplicación de esta metodología, y no pueden ser consideradas como un criterio emitido por el INAI. Más aún, el Pleno del Instituto no ha emitido criterios institucionales al respecto, además de que ciertos datos personales que en principio no se consideran sensibles, podrían llegar a serlo dependiendo del contexto en que se trata la información.

En virtud de lo anterior, se advierte que este Centro trata datos de nivel de riesgo inherente bajo y medio, al tratarse de datos:

- Datos identificativos;
- Datos electrónicos:
- Datos laborales;
- Datos afectivos y/o familiares;
- Datos patrimoniales;
- Datos fiscales;
- Datos sobre procedimientos administrativos y/o jurisdiccionales;

❖ Ciclo de vida de los datos:

- Obtención de los datos personales;
- Almacenamiento de los datos personales;
- 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;
- Divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
- Bloqueo de los datos personales, en su caso, y
- Cancelación, supresión o destrucción de los datos personales.

III.3 El valor y exposición de los activos involucrados en el tratamiento de los datos personales.

El INAI ha definido al activo, como todo elemento de valor para una organización, involucrado en el tratamiento de datos personales. Los activos se deben identificar

y ponderar con suficiente nivel de detalle para proveer información que permita hacer la valoración del riesgo.

Para efectos del presente, se manejarán tres tipos de activos:

❖ **Activos de información:**

- Datos personales recabados;
- Datos generados con motivo del tratamiento.

❖ **Activos Físicos:**

- Soportes de almacenamiento de datos físicos;
- Recursos Humanos.

❖ **Activos Tecnológicos:**

- Hardware;
- Software, y
- Redes y Telecomunicaciones.

III.4 Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida

El acceso a información personal derivado de una vulneración a los sistemas de seguridad con que cuenta el Centro podría tener como consecuencia negativa para los titulares:

• La afectación en la prestación de un servicio o trámite.

• El tratamiento de los datos para finalidades distintas a las establecidas en el Aviso de Privacidad, incluso, por un tercero.

• El cumplimiento de las finalidades para las cuales fueron recabados, de manera temporal o permanente.

III.5 Los factores:

Con base en lo previsto por el artículo 60, fracción V de los Lineamientos Generales, los factores a considerar en el análisis de riesgos son los señalados en el artículo 32 de la Ley General, esto es:

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.

a) El riesgo inherente a los datos personales tratados

La Metodología de Análisis de Riesgo BAA, señala que el responsable de los datos personales debe identificar los tipos de datos tratados, la sensibilidad de estos y el número de titulares para determinar el valor de riesgo inherente de los datos.

De igual forma, de acuerdo con la Metodología referida, el nivel de riesgo inherente se relaciona con la cantidad de personas de las cuales se tratan sus datos, cuyas cantidades van desde 1 hasta 500 mil, como fue expresado previamente.

Con base en estos elementos es dable considerar la relación del tipo de datos con el nivel de riesgo correspondiente, considerando el tipo de riesgo, el nivel inherente y el volumen de titulares.

Por ello, se estima conveniente retomar de la metodología en comento, los supuestos de riesgo inherente a los datos, adecuándose a aquellos con los que cuenta el Centro, a fin de que sirva de base para los sujetos responsables:

		Volumen de titulares				
Tipo de dato personal	**Nivel de riesgo inherente**	**<500**	**<5k**	**<50k**	**<500k**	**>500k**
Datos de Identificación	Bajo	1	1	1	1	1
Electrónicos	Bajo	1	1	1	1	1

Académicos	Bajo	1	1	1	1	1
Laborales	Bajo	1	1	1	1	1
De relaciones profesionales	Bajo	1	1	1	1	1
Fiscales	Medio	1	1	2	3	3
De relaciones comerciales	Medio	1	1	2	3	3
Sobre procedimientos administrativos y/o jurisdiccionales	Medio	1	1	2	3	3
Patrimoniales	Medio	1	1	2	3	3
Afectivos y/o familiares	Alto	2	2	3	3	3
Sobre movimientos migratorios	Alto	2	2	3	3	3
Sensibles	Alto	2	2	3	3	3
De salud	Alto	2	2	3	3	3
Menores	Alto Reforzado	4	4	5	5	5
Ubicación o domicilio particular en conjunto con datos de nivel medio o alto	Alto Reforzado	4	4	5	5	5

A continuación, se detallan los niveles mencionados:

❖ **Riesgo por tipo de dato Nivel 1, ocurre cuando**:

• El nivel de riesgo inherente de los datos sea bajo, sin importar el número de personas

• El nivel de riesgo inherente sea medio y se tengan hasta cinco mil (5,000) personas

• El nivel de riesgo inherente sea alto y se tengan hasta quinientas (500) personas

❖ **Riesgo por tipo de dato Nivel 2, ocurre cuando:**

• El nivel de riesgo inherente de los datos personales sea medio y se tengan hasta cincuenta mil (50,000) personas

• El nivel de riesgo inherente de los datos personales sea alto y se tengan hasta cinco mil (5,000) personas

❖ **Riesgo por tipo de dato Nivel 3, ocurre cuando:**

• El nivel de riesgo inherente de los datos personales sea medio y se tenga de cincuenta mil (50,000) personas en adelante

• El nivel de riesgo inherente de los datos personales sea alto y se tenga de cinco mil (5,000) personas en adelante

❖ **Riesgo por tipo de dato Nivel 4, ocurre cuando:**

• El nivel de riesgo inherente de los datos personales sea reforzado y se tengan hasta cinco mil (5000) personas

❖ **Riesgo por tipo de dato Nivel 5, ocurre cuando:**

• El nivel de riesgo inherente de los datos personales sea reforzado y se tengan más de cinco mil (5,000) personas.

La matriz de riesgos por inherencia a los datos personales tratados, así como por el volumen de titulares, forma parte del presente como Anexo 3.

b) La sensibilidad de los datos personales tratados;

Acorde con el inventario de datos que se anexa al presente, las áreas de este Centro que tratan datos personales reportan que no manejan datos personales sensibles.

c) El desarrollo tecnológico;

En la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados Comentada, se señala que, el desarrollo tecnológico "debe verse desde dos perspectivas: la inversión y sus consideraciones (deberá ir al menos relacionado con dos factores: el volumen de los datos personales y la sensibilidad de estos), así como la inversión y su alcance".

Asimismo, en dicha Ley comentada se establece que este elemento se cumple cuando el responsable implementa medidas que, desde el diseño, le permitan aplicar de forma efectiva el cumplimiento de los principios, deberes y demás obligaciones previstas en la normativa aplicable, en sus políticas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales.

Del mismo modo, las medidas técnicas y organizativas tomadas por el sujeto obligado o responsable deben ser apropiadas y orientadas a garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales estrictamente necesarios para cada uno de los fines específicos del tratamiento.

Con estas medidas de diseño y por defecto, se podrá generar un círculo virtuoso que conlleve a una efectiva protección de los datos personales, con lo cual se pueda cumplir, particularmente, con el principio de responsabilidad, como son:

1) Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y

2) Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia

d) Las posibles consecuencias de una vulneración para los titulares;

a) La destrucción no autorizada de la información o pérdida parcial que implique la afectación en la prestación de un servicio o trámite.

b) El acceso no autorizado que pueda conllevar al tratamiento de los datos para finalidades distintas a las establecidas en el Aviso de Privacidad, incluso, por un tercero.

c) La alteración o modificación de los datos que pueda impedir temporal o definitivamente el cumplimiento de las finalidades para las cuales fueron recabados.

e) Las transferencias de datos personales que se realicen;

Conforme al inventario de datos personales que forma parte del presente, los procesos en los cuales se puede realizar alguna transferencia de datos, son los siguientes:

Sujeto obligado receptor	**Datos**
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales	• Identificativos. • Electrónicos. • Académicos. • Laborales
De salud Autoridades judiciales	• Identificativos. • Laborales. • Patrimoniales. • Sensibles. • Sobre procedimientos administrativos y/o jurisdiccionales. • Afectivos y/o familiares.
Servicio de Administración Tributaria o	• Identificativos. • Laborales. • Patrimoniales

f) El número de titulares;

Respecto de este punto y conforme al tipo de datos personales que trata, el Centro se encuentra integrando la información relativa a los tratamientos de datos personales que realiza, en virtud de que algunas áreas se encuentran en un proceso de migración de información con fundamento en el artículo transitorio del Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Federal del Trabajo, de la Ley Orgánica del Poder Judicial de la Federación, de la

Ley de la Defensoría Pública, de la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores y de la Ley del Seguro Social, en materia de Justicia Laboral, Libertad Sindical y Negociación Colectiva, en el cual se señalan los lineamientos generales relacionados con el traslado de información al Centro.

g) Las vulneraciones previas ocurridas en los sistemas de tratamiento,

A la fecha no se ha registrado vulneración de datos.

h) 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.

Relativo al presente punto es conveniente retomar el cuadro plasmado en el punto III.1, inciso a) del presente apartado, en el cual se establece el riesgo de los datos, con base en los elementos siguientes:

- Tipo de datos tratados y
- Nivel de riesgo inherente.

Esto es, el valor que para un tercero representaría la obtención de los datos tratados por el Centro es proporcional al nivel de seguridad asignado, en donde tendrán mayor valía aquellos datos de menores o conjuntos, no sólo por el tipo de estos sino por el volumen de titulares involucrados.

III.6 Resultado del análisis de riesgos

Los retos institucionales para evitar acciones inesperadas que impliquen un riesgo en la protección de los datos personales son muchos; sin embargo, es necesario establecer estos con carácter preventivo.

Por ello, para el Centro es de gran interés fomentar en los recursos humanos con que cuenta, la importancia en la protección de datos personales y de su tratamiento, con el fin de prever, evitar o, en su caso, mitigar inmediatamente cualquier incidencia o vulneración a las bases de información personal con que cuenta, tanto físicas como electrónicas, por lo cual ha puesto énfasis en medidas físicas y técnicas para ello.

Lo anterior no es suficiente, pues el eslabón más débil en esta cadena de custodia o protección de los datos es el factor humano y, por tal motivo, resulta importante fortalecer las medidas de seguridad actuales, con el propósito de aminorar o nulificar cualquier riesgo que pudiera suscitarse.

En consecuencia, es recomendable fortalecer o implementar, en su caso, las medidas de seguridad siguientes:

❖ **Físicas**

• Instalación, reparación y/o modificación de sistemas de desagüe, a fin de impedir la filtración de agua a las oficinas en las cuales se encuentran almacenados los archivos.

• Cambio y/o instalación de cerraduras con reforzamiento.

• Mantenimiento de los sistemas de aire acondicionado, energía eléctrica u otros, a fin de prevenir el daño de los archivos.

❖ **Administrativas**

• Actualización de las disposiciones administrativas de carácter interno para la generación de copias de seguridad y respaldo de la información.

• Emisión de directrices dirigidas a los sujetos responsables para el borrado seguro de los datos.

• Armonización de las disposiciones internas con la Ley General de Archivos.

• Incremento de la capacitación focalizada a quienes intervienen en el tratamiento de los datos personales.

• Elaboración e implementación de guías, formatos o directrices para la detección y notificación de incidentes de seguridad.

❖ **Técnicas**

• Actualización de firmware y software para prevenir vulnerabilidades de origen.

• Implementación de técnicas de cifrado seguro de la información, acordes con los tratamientos de datos que se realizan.

• Gestión de soporte y mantenimiento a los sistemas con que cuentan los sujetos responsables y en los cuales se contengan datos personales.

IV. Análisis de brecha

El análisis de brecha es definido como “la concentración de elementos específicos que pueden existir entre lo deseable y lo actual, para ello es importante definir con

claridad cuál es la brecha que se desea analizar, identificar quiénes están involucrados, establecer cuáles son las causas más relevantes que determinan la brecha, identificar las diferencias de comportamiento entre los sistemas o actores a comparar en la brecha, identificar los indicadores y/o atributos de la situación actual y elaborar un listado con la finalidad de medir o caracterizar la brecha"

Esta definición nos permite aterrizar lo previsto en los Lineamientos Generales, en cuyo artículo 61 dispone que, en la realización del análisis de brecha, el responsable debe considerar:

1. Las medidas existentes y efectivas;

2. Las medidas de seguridad faltantes, y

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

Previo a referir tales puntos, es necesario establecer los tipos de medidas adoptadas por las áreas que integran el Centro y tratan datos personales, para garantizar la confidencialidad, integridad y disponibilidad de estos, las cuales se clasifican en: físicas, administrativas y técnicas.

Físicas. - Estas son definidas en el artículo 3, fracción XXII de la Ley General, como el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Para tal efecto, se deben considerar, al menos, las actividades siguientes:

a. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, a efecto de asegurar su disponibilidad e integridad.

Administrativas. – El artículo 3, fracción XXI de la Ley General, establece que son políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro

de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Técnicas. – Finalmente, las medidas técnicas se definen en el artículo 3, fracción XXIII de la Ley General, como el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades requeridas con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Establecido lo anterior, en las subsecuentes líneas se desglosará, grosso modo, lo establecido en el artículo 61 de los Lineamientos Generales, consistente en los elementos a considerarse para la elaboración del análisis de brecha, conforme a lo siguiente:

IV.1 Las medidas de seguridad existentes y efectivas

Para el tratamiento de los datos personales con que cuentan los sujetos responsables del Centro, se han establecido las medidas de seguridad, siguientes:

❖ **Físicas**

• Registro peatonal y vehicular a las instalaciones del sujeto obligado;

• Aviso a la vista con las restricciones del acceso a todo personal externo a las diferentes áreas de los sujetos responsables;

• Puertas de acceso a oficinas con llave;

• Archiveros con llave o candado;

• Sistemas contra incendios y en constante mantenimiento;

• Bitácoras de control de acceso a archivos, expedientes o sistemas que contienen datos;

• Áreas de almacenamiento de información exclusivos para el resguardo de datos personales, en soporte físico y/o electrónico;

• Alarmas contra inundaciones, incendios o sismos que permiten prevenir o mitigar un daño a los archivos.

❖ **Administrativas**

• Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en la cual se establecen los principios y deberes que rigen el tratamiento de los datos.

• Lineamientos Generales de Protección de Datos Personales para el Sector Público.

• Reglas de Integración y Funcionamiento de la Unidad de Transparencia y del Comité de Transparencia del Centro.

• Programa Anual de Capacitación en materia de transparencia, Acceso a la Información Pública, Accesibilidad y Protección de Datos Personales del Centro.

• Guía para el tratamiento de datos biométricos.

❖ **Técnicas**

• Cifrado de las redes inalámbricas que conforman la red interna del Centro.

• Uso de firmware y software con licencias.

• Control de permisos de usuarios de equipos de cómputo y redes.

IV.2 Las medidas de seguridad faltantes

Existen diversas acciones susceptibles de aplicarse, con el objeto de fortalecer las medidas de seguridad con que actualmente cuenta el Centro, las cuales se reiteran para mejor referencia:

❖ **Físicas**

• Cambio y/o instalación de cerraduras con reforzamiento.

• Mantenimiento de los sistemas de aire acondicionado, energía eléctrica u otros, a fin de prevenir el daño de los archivos.

❖ **Administrativas**

• Actualización de las disposiciones administrativas de carácter interno para la generación de copias de seguridad y respaldo de la información.

• Emisión de directrices dirigidas a los sujetos responsables para el borrado seguro de los datos.

• Armonización de las disposiciones internas con la Ley General de Archivos.

• Incremento de la capacitación focalizada a quienes intervienen en el tratamiento de los datos personales.

• Elaboración e implementación de guías, formatos o directrices para la detección y notificación de incidentes de seguridad.

❖ **Técnicas**

• Actualización de software para prevenir que contenga vulnerabilidades no corregidas por el fabricante.

• Actualización de firmware.

• Implementación de técnicas de cifrado seguro de la información, acordes con los tratamientos de datos que se realizan.

• Brindar soporte y mantenimiento a los sistemas con que cuentan los sujetos responsables y en los cuales se contengan datos personales.

Estas medidas faltantes o complementarias derivan de las actualmente implementadas y que han permitido un adecuado tratamiento de datos personales.

IV.3 La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente

• Digitalización de archivos.

• Implementación de sistemas biométricos para el resguardo o acceso a archivos.

• Instalación de centro de datos o de almacenamiento de datos alterno a la sede del Centro.

Las anteriores medidas de carácter físico y técnico tienen la finalidad de sistematizar la información, con el objeto de: eficientes los procedimientos realizados por los sujetos responsables, promover la gestión documental y garantizar el ciclo vital de los archivos, incrementar las medidas de control a documentación que contenga datos personales y, finalmente, prever cualquier afectación a los centros de datos que pudiera impedir su recuperación inmediata, parcial o total, al estar concentrados en la misma sede.

IV.4 Resultados del análisis de brecha

De lo referido hasta el momento en este punto, se puede desprender que, las medidas de seguridad implementadas por los sujetos responsables del Centro han posibilitado el resguardo efectivo de los datos personales tratados por cada uno de ellos y, a su vez, evitar incidentes.

No obstante, existe una brecha importante a considerar, la cual está enfocada, principalmente a la gestión documental, ciclo vital de los documentos y de los datos, la actividad archivística, así como con la capacitación focalizada, particularmente al personal de nuevo ingreso y que es designado para realizar, coordinar o supervisar el tratamiento de información de carácter personal.

Por tal motivo, lo idóneo para aminorar esta brecha es centrar esfuerzos en la armonización de la normativa actual a la de archivos y, a su vez, implementar acciones de capacitación permanente respecto de ambas materias: archivos y tratamiento de datos personales.

V. Plan de Trabajo

Una vez identificados los factores de riesgo, con los cuales se pueden ver comprometidos los datos personales objetos de tratamiento por parte de los sujetos responsables del Centro, y con la certeza de identificar a través del análisis de brecha, las medidas de seguridad faltantes para cumplir con la correcta protección que conlleve a garantizar la seguridad y confidencialidad, se presentan las acciones a desarrollar, conforme a lo siguiente:

1. Promover e impulsar la capacitación en materia de protección de datos personales a todos los sujetos responsables para abatir la falta de conocimiento por parte del personal de nuevo ingreso.

2. Identificar necesidades de capacitación en temas específicos en la implementación de la Ley General, como lo pueden ser: Obligaciones de la protección de datos personales; elaboración de avisos de privacidad y establecimiento de medidas de seguridad.
3. Aprobar el Programa General de Capacitación.
4. Proponer la implementación de políticas de traslado seguro de la información en la cual se contienen datos personales mediante medidas de seguridad que eviten la vulneración de la información.
5. Impulsar la generación de procesos de digitalización de información que contiene datos personales.
6. Sensibilizar sobre la importancia de la generación de copias de respaldo de la información que contiene datos personales para minimizar el posible daño por pérdida de estos por razones de causas naturales o casos fortuitos.
7. Actualizar el inventario de datos personales para la posible detección de nuevos tratamientos o la modificación de estos.
8. Promover la revisión periódica de las medidas de seguridad a efecto de identificar posibles deficiencias en sus procesos de implementación; para lo cual el sujeto responsable remitirá, por lo menos una vez al año, un informe al responsable designado conforme al art. 85 de la LGDPPSO, que dé cuenta de esta revisión.

En relación con lo anterior, a continuación, se presenta el Plan de Trabajo a desarrollarse:

ACCIÓN	ENCARGADO	TEMPORALIDAD
1	Unidad de Transparencia	Permanente
2	Unidad de Transparencia	Permanente
3	Comité de Transparencia	Anualmente
4	Unidad de Transparencia	Permanente
5	Área competente de archivo	Anualmente

6	Unidad de Transparencia y Tecnologías de la Información y Comunicaciones	Permanente
7	Unidad de Transparencia	Anualmente
8	Responsable designado conforme al art. 85 de la LGDPPSO y sujetos responsables	Permanente

Por la complejidad que representan algunos tratamientos de datos personales de este Centro, fue necesario llevar a detalle el análisis de riesgos, análisis de brecha y plan de trabajo, respecto de esos tratamientos.

VI. Mecanismos de monitoreo y revisión de las medidas de seguridad

Una de las acciones que todo sujeto obligado y responsable de los datos debe prever, son mecanismos de monitoreo y revisión de las medidas de seguridad implementadas, a fin de detectar áreas de mejora que le permitan fortalecer las existentes o implementar otras.

Por tal motivo, en el presente apartado se establecen las acciones a realizar por parte de los sujetos responsables que tratan datos personales y el responsable designado conforme al art. 85 de la LGDPPSO, con base en la atribución establecida para este órgano en el artículo 84, fracción V de la Ley General, consistente en supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad, lo cual se realizará acorde con lo siguiente:

VI. 1 Revisión y análisis de medidas de seguridad

Los titulares de los sujetos responsables que traten datos personales deberán revisar las medidas de seguridad implementadas para la protección de los datos personales recabados e informar, en los meses de enero y julio al responsable designado conforme al art. 85 de la LGDPPSO lo siguiente:

a) Los nuevos activos que se incluyan en la gestión de riesgos;

b) Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;

c) Las nuevas amenazas que podrían estar activas, internas y/o externas, y que no han sido valoradas;

d) La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;

e) Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

f) El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo;

g) Los incidentes y vulneraciones de seguridad ocurridas;

h) Las acciones realizadas para la implementación o actualización de las medidas de seguridad, y

i) La actualización, modificación o supresión de bases de datos, en su caso.

El responsable designado conforme al art. 85 de la LGDPPSO podrá solicitar al Comité de Transparencia la aprobación de medidas, recomendaciones o criterios a los sujetos responsables, con el objeto de fortalecer las acciones implementadas para el adecuado tratamiento de los datos personales.

VI.2 Auditorías

Acorde con lo establecido en los artículos 151 de la Ley General y 218 de los Lineamientos Generales, la Unidad de Transparencia a través del Comité de Transparencia, podrá solicitar la realización de una auditoría al INAI, con el objeto de verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable.

VI.3 Sistema de Gestión

Será a través del sistema de gestión que, los sujetos responsables planifiquen, implementen, monitoreen y mejoren de manera continua las medidas de seguridad

administrativas, físicas y técnicas, conforme a lo establecido en la normatividad aplicable.

En este sentido, el enlace del sujeto responsable deberá monitorear y revisar las medidas de seguridad, supervisando lo siguiente:

- Nuevos activos gestionados
- Modificaciones necesarias
- Nuevas amenazas
- Posibilidad de nuevas vulneraciones
- Impacto de las amenazas valoradas, vulnerabilidades y riesgos
- Incidentes y vulneraciones de seguridad ocurridas.

VII. Programa General de Capacitación en materia de datos personales

A fin de dar cumplimiento a esta obligación, el Centro, a través del Comité de Transparencia, deberá aprobar anualmente el Programa de Capacitación Institucional que al efecto someta a consideración de este colegiado la Unidad de Transparencia, el cual deberá contemplar la materia de datos personales y, prever, al menos los temas siguientes:

- Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Principios que regulan el tratamiento de datos personales, deberes y obligaciones de los sujetos responsables.
- Inventario de Datos Personales.
- Elaboración de Avisos de Privacidad (integral y simplificado)
- Medidas de seguridad orientadas a la protección, seguridad y confidencialidad en el tratamiento de datos personales

En su integración deberán considerarse diversas fechas para la impartición de los cursos, los roles del personal involucrado en el tratamiento de datos personales y las áreas a las que estos corresponden.

Dicho programa deberá ser difundido por responsable designado conforme al art. 85 de la LGDPPSO, a todos los sujetos responsables del Centro.

El Programa de Capacitación podrá prever la impartición de cursos a través del personal con que cuenta la Unidad de Transparencia o el de los sujetos

responsables, así como de aquella proporcionada por el INAI o cualquier otra instancia del sector público o privado.

VIII. Aprobación y Difusión del Documento de Seguridad

El presente documento de seguridad es aprobado por el Comité de Transparencia, acorde con las atribuciones previstas en los artículos 84, fracciones I y V de la Ley General, así como 10, fracciones VI y XX de las Reglas de Integración y Funcionamiento de la Unidad de Transparencia y del Comité de Transparencia del, mismos que son del tenor literal siguiente:

> ***"artículo 84****. Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, el Comité de Transparencia tendrá las siguientes funciones:*
>
> I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;
>
> […]
>
> V. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
>
> ***"Artículo 10****. Además de las atribuciones que establecen los artículos 65 de la Ley Federal, y 43 de la Ley General el Comité tendrá las que a*
>
> *continuación se señalan: Además de las funciones señaladas en los artículos 44 de la Ley General, 65 de la Ley Federal y 84 de la Ley General, el Comité de Transparencia tendrá las siguientes atribuciones:*
>
> *[…]*
>
> *VI. Vigilar el cumplimiento de las políticas, criterios, reglas, lineamientos y demás disposiciones normativas que emita el propio Comité y las autoridades competentes en la materia:*
>
> *[…]*
>
> *XX. Las demás que le confieran la Ley Federal y la Ley General"*

Cualquier modificación al presente documento de seguridad y sus anexos, deberá ser aprobada por el Comité de Transparencia, conforme a los supuestos establecidos en el siguiente apartado.

Asimismo, este documento deberá ser difundido por el responsable designado conforme al art. 85 de la LGDPPSO o quien este designe, a las personas titulares de los sujetos responsables quienes a su vez lo harán del conocimiento del personal a su cargo, debiendo recabar constancia de ello y resguardarla en sus archivos. Adicionalmente, el presente se publicará en la página de Internet del Centro.

No obstante lo anterior y en virtud de que la información contenida en el presente documento de seguridad fue proporcionada por los Enlaces de las áreas del Centro, serán ellos los facultados para decidir sobre el tratamiento de los datos personales, observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, además deberán sujetarse a las facultades o atribuciones que la normatividad aplicable les confiera y dar cabal cumplimiento a los Principios y Deberes, contenidos en el TÍTULO SEGUNDO, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En este sentido, la autorización del Comité de Transparencia del Centro está encaminada a dotarlo de las herramientas necesarias que promuevan el correcto tratamiento de los datos personales que manejan las áreas, sin sustituir en ningún momento las responsabilidades y deberes de los responsables, quienes tendrán la obligación de tomar todas las medidas necesarias para dar exacto cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

IX. Actualización Del Documento De Seguridad

El presente documento de seguridad podrá ser modificado cuando ocurra alguno de los eventos establecidos en el artículo 36 de la Ley General, siendo estos, los siguientes:

- 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, o
- Derivado de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Para tal efecto, el enlace de cualquiera de las áreas que se encuentre en alguno de los supuestos referidos solicitará por escrito al responsable designado conforme al art. 85 de la LGDPPSO las modificaciones respectivas, quien a su vez solicitará al Comité de Transparencia resolver lo conducente.

Adicionalmente, el documento de seguridad podrá ser actualizado cada cinco años, con motivo del cambio de direccion general de conformidad con el artículo 47 de la Ley Orgánica del Centro de Conciliación Laboral del Estado de Querétaro.

Las actualizaciones realizadas al documento de seguridad y sus anexos, serán publicados en los términos descritos en el apartado inmediato anterior y difundidos al personal que labora o presta sus servicios en el Centro.