ASEA
AGENCIA DE SEGURIDAD, ENERGÍA Y AMBIENTE

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

AGENCIA NACIONAL DE SEGURIDAD INDUSTRIAL Y DE PROTECCIÓN AL MEDIO AMBIENTE DEL SECTOR HIDROCARBUROS

CONTENIDO

Marco Normativo .....

Consideraciones .....

Objetivo del Documento de Seguridad .....

Funciones y obligaciones de las personas que traten datos personales .....

Análisis de Riesgo, análisis de brecha y plan de trabajo.....

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

Programa de Capacitación .....

MARCO NORMATIVO

Constitución Política de los Estados Unidos Mexicanos, artículo 6 y artículo 16 segundo párrafo.

Ley General de Transparencia y Acceso a la Información Pública

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

CONSIDERACIONES

La protección de los datos personales es un derecho humano consagrado en los artículos 6, apartado A y 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos.

Que todas las disposiciones de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General) son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal.

Que entre los objetivos de la Ley General se encuentra garantizar la observancia de los principios de protección de datos personales, proteger los datos personales en posesión de cualquier autoridad, así como promover, fomentar y difundir una cultura de protección de datos personales.

Que la Ley General define el documento de seguridad como el 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.

Que la Unidad de Transparencia tiene entre sus facultades asesorar a las unidades administrativas de la ASEA en materia de protección de datos personales, conforme a lo señalado en el artículo 85 de la Ley General.

Que el presente Documento de Seguridad se elabora en cumplimiento a lo dispuesto por el artículo 35 de la Ley General, señalando el control interno relacionado con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales que se recaban en la ASEA.

OBJETIVO

Adoptar las medidas de seguridad de carácter administrativo, físico y técnico, conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad para la protección de datos personales en atención a los sistemas de gestión de seguridad de la información de datos personales, garantizando el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, con el fin de protegerlos contra el daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado, garantizando un adecuado tratamiento de los datos personales,

FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

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

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

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

Funciones y obligaciones

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

De conformidad con lo anterior, las funciones y obligaciones de las personas servidoras públicas de la que, en el ejercicio de sus atribuciones, traten datos personales, deberán garantizar su confidencialidad, integridad y disponibilidad, dando cumplimiento a las obligaciones que se enlistan a continuación:

a) Observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

b) Tratar los datos personales para finalidades concretas, lícitas, explícitas y legítimas en ejercicio a las facultades o atribuciones que la normatividad aplicable les confiera.

c) Evitar la obtención y tratamiento de datos personales a través de medios engañosos o fraudulentos.

d) Tratar los datos personales previo consentimiento, expreso o tácito, otorgado por el titular de manera libre, específica e informada; salvo cuando se actualice alguna de las causales de excepción previstas en el artículo 22 de la LGPDPPSO.

e) Obtener el consentimiento expreso y por escrito del titular para su tratamiento, tratándose de datos personales sensibles, salvo en los casos previstos en el artículo 22 de la LGPDPPSO.

f) Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión a fin de que no se altere la veracidad de éstos.

g) Suprimir, previo bloqueo, los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad

h) Informar al titular, a través del aviso de privacidad, que deberá ser difundido por medios electrónicos y físicos, la existencia, características principales y finalidades del tratamiento al que serán sometidos sus datos personales.

I) Establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

j) Informar a la Unidad de Transparencia cualquier vulneración por personas no autorizadas respecto de las bases de datos personales en su poder.

k) Evitar realizar transferencia de datos personales, salvo que se cuente con el consentimiento de las y los titulares, o bien, cuando se actualice alguna de las excepciones previstas en los artículos 22, 66 y 70 de la LGPDPPSO.

l) Atender, dentro de los plazos establecidos, las solicitudes de ejercicio de los derechos ARCO que les sean turnadas por la Unidad de Transparencia.

ANÁLISIS DE RIESGO, ANÁLISIS DE BRECHA Y PLAN DE TRABAJO

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

> ***Artículo 33.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> ***I.*** *[…]*
> ***IV.*** *Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*

> ***V.*** *Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*
> ***VI.*** *Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*
> *[…]*

Como se señaló, de acuerdo con las fracciones III, IV y V del artículo 35 de la Ley General, los análisis de riesgo y brecha y el plan de trabajo forman parte del documento de seguridad.

Por su parte, los artículos 60, 61 y 62 de los Lineamientos Generales establecen lo siguiente:

Análisis de riesgos

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

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

Análisis de brecha

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

I. *Las medidas de seguridad existentes y efectivas;*
II. *Las medidas de seguridad faltantes, y*
III. *La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.*

Plan de trabajo

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

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

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

> ***Artículo 32.*** *Las medidas de seguridad adoptadas por el responsable deberán considerar:*
> *I. El riesgo inherente a los datos personales tratados;*
> *II. La sensibilidad de los datos personales tratados;*
> *III. El desarrollo tecnológico;*
> *IV. Las posibles consecuencias de una vulneración para los titulares;*
> *V. Las transferencias de datos personales que se realicen;*
> *VI. El número de titulares;*
> *VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y*
> *VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.*

A partir de lo dispuesto por los artículos antes citados, el análisis de riesgo se lleva a cabo a partir de cuatro fuentes de información:

1. Análisis de riesgos de la infraestructura tecnológica y recursos de software y hardware;
2. Análisis de riesgos de hábitos de seguridad del personal de la ASEA;
3. Análisis de riesgos a partir de los inventarios de tratamientos de datos personales, y
4. Análisis de riesgos vinculado con el cumplimiento de obligaciones normativas en materia de datos personales.

Los dos primeros análisis se realizan de manera general y aplican transversalmente, ya que el primero refiere a los distintos sistemas o medios en los que se llevan a cabo los diversos tratamientos que realiza la ASEA, por lo que los riesgos y controles que se determinen aplican de manera directa a estos medios o sistemas; mientras que el segundo versa sobre los hábitos de seguridad del personal, de manera general y no asociados a un tratamiento en lo particular.

Por su parte, los análisis 3 y 4 se realizan, de manera específica, asociados a cada uno de los tratamientos, y tomando en cuenta sus particularidades.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

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

Como se señaló, de acuerdo con la fracción VI del artículo 35 de la Ley General, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

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

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

Mecanismos de monitoreo

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

En ese sentido, los mecanismos de monitoreo son parte sustancial de la verificación de la efectividad del Sistema de Gestión de Seguridad de la Información de datos personales, por ello, se realizarán

acciones de monitoreo y supervisión de manera periódica en el momento que existan cambios relevantes en lineamientos legales, tecnologías, políticas o cualquier otro cambio que impacte dicho sistema, para lo cual, se deben revisar y registrar, al menos, algunos de los siguientes puntos, durante la fase de monitoreo del sistema:

1. Política de Seguridad de la Información.
2. Retroalimentación de usuarios y partes interesadas.
3. Herramientas, técnicas, métodos, etc., para la mejora del desempeño y efectividad del sistema.
4. Estado de las acciones correctivas y preventivas y eventos registrados de seguridad (incidentes).
5. Vulnerabilidades y/o amenazas no contempladas en el más reciente análisis de riesgo.
6. Acciones de seguimiento a compromisos de revisiones previas.
7. Cualquier cambio que pudiera afectar al sistema.
8. Recomendaciones para la mejora del sistema.

Mecanismos de supervisión o revisión

Además del monitoreo señalado anteriormente, se requiere realizar una supervisión periódica de las medidas de seguridad, a través de auditorías, las cuales pueden ser internas (desarrolladas por la propia ASEA) o externas (solicitando auditorías voluntarias al INAI).

Hasta el momento no se han realizado auditorías específicas en materia de protección de datos personales a los tratamientos de la ASEA.

El programa de auditoría será aquél que determine el Comité de Transparencia en el Programa de Protección de Datos Personales de la ASEA.

Programa de Capacitación

Se deberá establecer anualmente un programa de capacitación y actualización en materia de protección de datos personales, mismo que se integrará al Programa de Capacitación en Transparencia, Acceso a la Información, Protección de Datos Personales y Temas Relacionados.

Se realizará la detección de necesidades de capacitación, que integre los requerimientos de las personas servidoras públicas dependiendo de los roles y responsabilidades respecto del tratamiento de datos personales.

Para cumplir con lo antes señalado, se llevará a cabo la capacitación al personal de ASEA a cargo del tratamiento de Datos Personales a través del siguiente Programa de Capacitación en Materia de Protección de Datos Personales.

Para llevar a cabo la capacitación en algunos cursos en materia especializada se deberán cumplir algunos prerrequisitos definidos por la Dirección General de Capacitación del INAI, los cuales estarán

señalados en la oferta de capacitación emitida por el Instituto, y será dirigida a atender necesidades sobre aspectos particulares de la normatividad en materia de datos personales; asimismo, se determinará con base en las necesidades y funciones de cada una de las áreas que realizan el tratamiento de datos personales.

Los cursos serán impartidos por el INAI conforme a la oferta programada por la Dirección General de Capacitación y podrán realizarse en el modelo Presencial o Presencial a Distancia.