Políticas Internas de Gestión y Tratamiento de Datos Personales

OBJETIVO

Establecer las políticas en materia de protección de datos personales en los procesos internos de gestión y tratamiento de datos personales de la Agencia Nacional de Seguridad Industrial y de Protección al Medio Ambiente del Sector Hidrocarburos, conforme a lo previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos de Protección de Datos Personales para el Sector Público.

ÁMBITO DE APLICACIÓN

El presente documento es de aplicación y observancia general y obligatoria para todas las personas servidoras públicas de la ASEA que conforme a sus atribuciones realicen tratamiento de datos personales.

DISPOSICIONES GENERALES

1. Se realizará el tratamiento de datos personales con base en las atribuciones conferidas a cada una de las áreas de la ASEA dentro del marco legal en la materia y del consentimiento de la persona titular.

2. Previo a recabar datos personales, se debe mostrar el aviso de privacidad integral y/o simplificado, según sea el caso; el aviso de privacidad debe encontrarse en un lugar visible y se deberá hacer del conocimiento de la persona titular la finalidad con la cual se reciben.

3. Las áreas solo deberán tratar los datos personales que resulten estrictamente necesarios para el ejercicio de atribuciones y funciones.

4. Se deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que se reciban en ejercicio de las atribuciones otorgadas a las áreas de la ASEA.

5. Es obligación de todas las personas servidoras públicas de la ASEA que administren, actualicen o tengan acceso a bases de datos personales, conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros.

6. Las áreas deberán identificar todos los avisos de privacidad que se requieren, según los tratamientos que realicen.

7. Los avisos de privacidad deberán ser elaborados en sus dos modalidades: simplificado e integral y contener todos los elementos informativos que exige la norma, además de estar redactados de manera clara y sencilla.

8. Las áreas deberán verificar que sus avisos de privacidad simplificados e integrales se encuentren publicados en el portal de internet de la ASEA.

PRINCIPIOS, DEBERES Y OBLIGACIONES

Principio de licitud.

Los datos personales tienen que ser tratados de manera lícita, esto es, debe sujetarse a las facultades o atribuciones que la normatividad aplicable le otorga.

Las áreas deberán ajustarse a las siguientes recomendaciones:

1. Revisar que los datos se traten conforme a la LGPDPPSO, Lineamientos Generales de Protección de Datos Personales para el Sector Públicos y demás normativa aplicable.
2. Conocer la normativa que en lo particular regule sus atribuciones, funciones y responsabilidades con relación al tratamiento de los datos personales que realice.

Principio de lealtad.

La obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos.

Las áreas deberán revisar los procedimientos y formatos utilizados para recabar datos personales, para verificar que en éstos no se utilicen prácticas que lleven a la obtención de los datos de manera dolosa, de mala fe o con negligencia, tratar los datos conforme lo acordado e informado a la persona titular de los datos personales.

Principio del consentimiento.

Las áreas que realicen tratamiento de datos personales deberán contar con el consentimiento del titular para el tratamiento de sus datos personales, el cual deberá ir siempre ligado a las finalidades concretas del tratamiento que se informen en el aviso de privacidad.

Las áreas deberán identificar las finalidades para las cuales se requiere el consentimiento de los titulares y solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad, así como, definir el tipo de consentimiento que se requiere, según las categorías de datos personales que se vayan a tratar o las disposiciones normativas que regulen el tratamiento.

Principio de información.

Las áreas que realizan tratamientos de datos personales se encuentran obligadas a informar a las personas titulares de los datos personales, a través de los avisos de privacidad integral y simplificado, las características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Las áreas deberán poner a disposición el aviso de privacidad en sus dos modalidades, simplificado e integral en el portal de internet de la ASEA.

Deber de seguridad

Este deber consiste en establecer las medidas de seguridad de carácter administrativo, físico y técnico que resulten necesarias para la protección de los datos personales, protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Las áreas deberán adoptar las medidas de seguridad administrativas, físicas y técnicas que resulten necesarias acorde al riesgo inherente a los datos personales tratados, la sensibilidad de los datos personales tratados, las posibles consecuencias de una vulneración para los titulares, las transferencias de datos personales que se realicen, el número de titulares, las vulneraciones previas ocurridas en los sistemas de tratamiento, así como el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada. Deberán monitorear y revisar de manera periódica la efectividad de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

Deber de confidencialidad.

Para cumplir con este deber es necesario establecer acciones que tengan por objeto que todas aquellas personas servidoras públicas que intervengan en el tratamiento de los datos personales guarden confidencialidad respecto de éstos, aún después de que éstas causen baja laboral.

Las áreas deberán implementar los mecanismos necesarios para que el personal que intervenga en el tratamiento de datos personales se comprometa a guardar confidencialidad sobre los mismos, lo anterior incluso después de finalizar su relación con la ASEA, capacitar al personal para que conozca sus obligaciones con relación al tratamiento de datos personales y establecer procedimientos para evitar fuga de información o el acceso indebido a los datos personales.

ROLES Y RESPONSABILIDADES

Con relación a lo dispuesto en el artículo 33, fracción II de la LGPDPPSO, 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.

Personas servidoras públicas de la ASEA

Las personas servidoras públicas 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.

SANCIONES POR INCUMPLIMIENTO A LAS DISPOSICIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES.

Serán causas de sanción por incumplimiento de las obligaciones en materia de protección de datos personales, las establecidas en el artículo 163 de la LGPDPPSO:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO.
II. Incumplir los plazos de atención previstos en la LGPDPPSO para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate.
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO.
V. No contar con los avisos de privacidad, o bien, omitir en los mismos alguno de los elementos a que se refieren los artículos 27 y 28 de la LGPDPPSO.
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se 19 cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.
VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de LGPDPPSO
VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO.
IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la LGPDPPSO.
X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO.
XI. Obstruir los actos de verificación de la autoridad.
XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO.

CICLO DE VIDA DE LOS DATOS PERSONALES

Cuando se obtengan datos personales, las Áreas deberán identificar el ciclo de vida de dichos datos, lo anterior conforme a las particularidades de cada tratamiento, pero, en cualquier caso, considerando las siguientes etapas: Las áreas deberán identificar el riesgo inherente de los datos personales, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software, personal, o cualquier otro recurso humano o material que resulte pertinente considerar.

Para identificar el ciclo de vida de los datos personales se deberá elaborar un inventario considerando los siguientes elementos: medios a través de los cuales se recaban los datos

personales, en qué procesos se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimirán

PROCESO GENERAL PARA EL ESTABLECIMIENTO, ACTUALIZACIÓN, MONITOREO Y REVISIÓN DE LOS MECANISMOS Y 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. 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.

Las acciones de monitoreo y supervisión periódica para las medidas de seguridad que se implementarán en la ASEA serán los siguientes:

Mecanismos de Monitoreo

Para los tratamientos de datos personales de la ASEA, se consideran los siguientes tipos de monitoreo:
1) Revisión de cumplimiento de las políticas internas, relacionadas con el tratamiento de datos personales. Tiene el objetivo de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la Ley General, los Lineamientos Generales, y demás normatividad que resulte aplicable.
2) Revisión del riesgo, tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, ya sea dentro del entorno físico o bien el entorno electrónico
3] Actualización del plan de trabajo. Derivado del monitoreo del entorno físico o electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados.

Mecanismos de supervisión o revisión

Además del monitoreo continuo de las medidas de seguridad, 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 (Realizadas por el INAI). Así, respecto del programa de auditoría mencionado en el último párrafo del artículo 63 de los Lineamientos Generales, se tiene contemplada la realización de una auditoría en materia de protección de datos personales, al menos una vez al año.