DICONSA

Sistema de Supervisión y Vigilancia de Diconsa S.A. de C.V.

Índice

I. Introducción

A. El artículo 29, de la Ley General De Protección De Datos Personales en Posesión de Sujetos Obligados, establece que "…el responsable deberá implementar los mecanismos previstos en el artículo 30 de la presente ley para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la presente ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular e instituto o a los organismos garantes, según corresponda, caso en el cual deberá observar la constitución y los tratados internacionales en los que el estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.

B. El artículo 30, fracción V de mencionada ley, establece que entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad es "…establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales…"

C. El artículo 33, fracción VII, de la Ley General, dispone que se deberán de monitorear y revisar de manera periódica los aspectos siguientes:

- Las medidas de seguridad implementadas en la protección de datos personales.
- Las amenazas y vulneraciones a que están sujetos los tratamientos o sistemas de datos personales.

D. Asimismo, el artículo 49 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, establece que el responsable deberá revisar las políticas y programas de seguridad y el sistema de supervisión y vigilancia implementado, al menos, cada dos años, salvo que realice modificaciones sustanciales a los tratamientos de datos personales que lleven a cabo y, en consecuencia, amerite una actualización previa al plazo establecido en el presente artículo.

E. De igual forma, el artículo 63 de los citados Lineamientos establece que 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.

II. Marco Jurídico

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Acuerdo mediante el cual se aprueban los Instrumentos Técnicos que refiere el Titulo Decimo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

III. Definiciones

Instituto: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados.

Titular: La persona física a quien corresponden los datos personales.

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

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.

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 políticas y preferencia sexual.

IV. Sistema de Supervisión y Vigilancia

De conformidad con lo establecido en los artículos 29 y 30, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 49 de los Lineamientos Generales de Protección de Datos Personales para el sector público, se realizan de manera periódica supervisiones y vigilancia a las áreas administrativas que integran de este Sujeto Obligado, como sigue:

a) Supervisar que las medidas de seguridad de carácter físico, técnico y administrativo, protejan los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad e impedir que cualquier tratamiento contravenga las disposiciones del marco normativo en la materia.

b) Supervisar que la capacitación del personal, se realice apegándose a lo establecido en Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

c) Vigilar con estricta observancia a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, en el tratamiento de los datos personales.

d) Supervisar que las 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 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

e) Supervisar que los datos personales obtenidos, se conserven y se traten bajo la más estricta confidencialidad.

f) Supervisar que los tratamientos de datos personales que lleva a cabo este sujeto obligado, no den lugar a la discriminación, trato injusto o arbitrario en contra del titular.

g) Supervisar que los datos personales que se recaben, sean los adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento.

h) Supervisar que los avisos de privacidad se coloquen en lugares visibles que faciliten la consulta del titular.

i) Supervisar que los avisos de privacidad integrales se encuentren de manera permanente en el portal de internet de este sujeto obligado.

j) Verificar que las personas con algún tipo de discapacidad o grupos vulnerables, puedan ejercer en igualdad de circunstancias su derecho a la protección de datos personales.

k) Supervisar que las solicitudes de ejercicio de derechos ARCO sean tratadas de conformidad a lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público, en relación a los requisitos, prevenciones, costos, modalidades de entrega, incompetencias, negativas, tramites específicos y acreditación de la identidad, de los menores de edad, personas con incapacidad legal o estado de interdicción, ejercicio de derechos de personas fallecidas, de los titulares o sus representantes debidamente identificados y acreditados.

l) Supervisar que los mecanismos que se lleven a cabo para la entrega de la información, aseguren que los datos personales solo se entreguen al titular o en su caso, al representante debidamente acreditado. Asimismo, se informe al titular el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables.

Para cumplir con lo anterior, se indica a las áreas administrativas que deberán poner especial atención a lo siguiente:

- ✓ Deberán realizar un monitoreo constante que les permita detectar amenazas nuevas, que podrían estar activas dentro y fuera de su área y que anteriormente no habían sido detectadas.

- ✓ Llevarán a cabo acciones para dar seguimiento y monitoreo a las vulnerabilidades existentes y estar en condiciones de detectar las que se encuentran expuestas a nuevas amenazas.

- ✓ Cuando en su gestión de riesgos (en caso de que lo elaboren), se incluyan nuevos activos, realizar las actualizaciones previo monitoreo, considerando las modificaciones necesarias a los activos, por ejemplo, si existe algún cambio o migración tecnológica, entre otras.

- ✓ Deberán monitorear y realizar los cambios pertinentes en el impacto o consecuencias de amenazas, vulnerabilidades y riesgos que hayan sido detectadas con anticipación, que pudieran considerarse con un nivel inaceptable de riesgo.

Las áreas administrativas, deben contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

La Unidad de Transparencia de la Entidad, será la encargada de ejecutar los mecanismos de monitoreo y supervisión de las medidas de seguridad implementadas por la misma Unidad de Transparencia, así como, por las áreas administrativas, en la protección de datos personales, a través de los siguientes ejes:

Etapa de Monitoreo.

La Unidad de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales, a través de sus inventarios, la elaboración de un reporte, en el que deberá precisarse, lo siguiente:

1. Si se elaboraron los avisos de privacidad.
2. Si se ha definido y establecido medidas de seguridad administrativas, técnicas y físicas.
3. Si se ha revisado el marco normativo que regula el tratamiento de datos personales.
4. Si se contemplan medidas de seguridad específicas o adicionales.
5. Si se han definido las funciones, obligaciones de cada servidor público que trata datos personales.
6. Si se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando durante el tratamiento de datos personales.
7. Si se ha elaborado el inventario de datos; el análisis de riesgo; así como el análisis de brecha.
8. Si se monitorean y revisan de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones.

Etapa de Supervisión.

A. La Unidad de Transparencia analizará los reportes de las áreas administrativas, verificando aquellos puntos en los que se hubiera reportado "No" como respuesta y se emitirá un dictamen o ficha técnica en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas las atiendan y remitan las evidencias de su cumplimiento.

B. La Unidad de Transparencia deberá monitorear y revisar de manera periódica las medidas de seguridad, así como las amenazas y vulneraciones a las que están sujetos los datos personales, para lo cual se podrá auxiliar de las personas designadas por las áreas administrativas como responsables en el tratamiento de datos personales, personal especialista en Tecnologías de la Información, así como, personal que haya recibido alguna capacitación en la materia.

C. Asimismo, citada unidad debe contar con un mecanismo que permita monitorear las alertas de seguridad de los datos personales, como posibles incidentes de seguridad.

D. De acuerdo a lo estipulado en el artículo 30, fracción V, de la Ley General de Datos Personales en Posesión de Sujetos Obligados, se establece que debe mantenerse un sistema de supervisión y vigilancia, incluyendo auditorías, que permitan comprobar el cumplimiento de las políticas de datos personales.

E. De igual forma, el artículo 63 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales), dispone que además del monitoreo y supervisión periódica de las medidas de seguridad, se deberá contar con un programa de auditoría para revisar la eficacia y eficiencia del sistema de gestión.

F. Se programarán auditorías en materia de datos personales a las áreas administrativas, buscando las finalidades siguientes:

- ✓ Verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

- ✓ Analizar el cumplimiento de los deberes y principios en los tratamientos de los datos personales que fueron documentados a través de los inventarios por cada una de las áreas, por lo que, la Unidad de Transparencia propondrá al Comité de Transparencia la programación por inventario y, el deber o principio que deberá ser objeto de la auditoría.

Lo anterior, permitirá identificar de forma ordenada las acciones y mejoras que habrán de implementarse para el adecuado manejo y protección de los datos personales.

V. Conclusión

Las actividades de supervisión y vigilancia que lleva a cabo este Sujeto Obligado a las áreas administrativas que lo integran, tiene por objeto verificar que los procedimientos que se implementan, garanticen y aseguren la protección a los datos personales de conformidad a lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Así mismo, verificar y analizar el cumplimiento de los deberes y principios en los tratamientos de los datos personales que fueron documentados a través de los inventarios que manifestaron las áreas administrativas en cumplimiento de las disposiciones normativas en la materia.