SISTEMAS DE SUPERVISIÓN Y VIGILANCIA EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN EL INSTITUTO MEXICANO DE LA RADIO

INTRODUCCIÓN

El artículo 30, fracción V, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establece que, entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el de implementar un sistema de supervisión y vigilancia, que permita comprobar el cumplimiento de las políticas de protección de datos personales. En ese sentido, el artículo 35, fracción VI, de la Ley General establece que el documento de seguridad deberá contener, entre otros aspectos, los mecanismos de monitoreo y revisión de las medidas de seguridad. Al respecto, el artículo 33, fracción VII, de la Ley General, dispone que se deberán de monitorear y revisar de manera periódica los aspectos siguientes:

1. Las medidas de seguridad implementadas en la protección de datos personales.
2. Las amenazas y vulneraciones a que están sujetos los tratamientos o sistemas de datos personales En ese contexto, el artículo 63 de los Lineamientos Generales de protección de datos personales para el sector público 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. Para cumplir con lo anterior, se deberá monitorear continuamente lo siguiente:

1. Los nuevos activos que se incluyan en la gestión de riesgos.
2. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.
3. Las nuevas amenazas que podrían estar activas dentro y fuera del sujeto obligado y que no han sido valoradas.
4. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
5. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.
6. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
7. Los incidentes y vulneraciones de seguridad ocurridos.

En ese sentido, el Instituto Mexicano de la Radio desarrollará el cumplimiento de dicha obligación a través de un mecanismo de monitoreo y supervisión; y el Mecanismos de actuación ante vulneraciones a la seguridad de los datos personales.

GLOSARIO

Mecanismo: Proceso sistemático y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para el monitoreo a los sistemas de datos personales del IMER

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 los mismos.

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.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública, autoridad máxima en materia de protección de datos personales.

IMER: Instituto Mexicano de la Radio.

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.

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

Documento de Seguridad: 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.

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.

Incidente: Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas del IMER, que afecte la confidencialidad, la integridad o la disponibilidad de los datos personales. LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

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

Medidas de seguridad: El conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger la información en posesión del IMER.

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.

Programa: Programa de Protección de Datos Personales.

Responsable del tratamiento de datos personales: IMER a través de sus unidades administrativas.

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.

Servidor público: El o los servidores públicos de las unidades administrativas, encargados del tratamiento de datos personales.

Sujeto obligado: Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, del ámbito federal.

Titular: La 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: Las Unidades Administrativas del IMER previstas en el Estatuto Orgánico y que traten o puedan tratar datos personales.

Unidad de Transparencia: La instancia a la que hace referencia el artículo 85 de la Ley General.

Vulnerabilidad: La circunstancias o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño.

Vulneración de seguridad: El incidente de seguridad que afecta a los datos personales en cualquier fase de su tratamiento.

AMBITO DE APLICACIÓN

Las directrices contenidas en el presente documento son de aplicación general para las personas servidoras públicas que integran las unidades administrativas adscritas al IMER que, en el ejercicio de sus funciones, obtengan, usen, registren, organicen, conserven, elaboren, utilicen, comuniquen, difundan, almacenen, posean, manejen, aprovechen, divulguen, transfieran o dispongan de datos personales.

DISPOSICIONES GENERALES

A fin de corroborar el cumplimiento del programa y de las políticas de protección de datos personales, los tratamientos de datos personales, la verificación, la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados por el IMER para el cumplimiento de las obligaciones previstas en la LGPDPPSO; así como en los Lineamientos Generales y demás normatividad aplicable en la materia, se establece el siguiente mecanismo:

Mecanismo para el Monitoreo y Supervisión

El Comité de Transparencia acordará por unanimidad, se realice el monitoreo a los sistemas de datos personales del IMER, mismo que se llevarán a cabo cada semestre durante el mes de enero y julio con el objeto de comprobar el cumplimiento de las obligaciones previstas en la LGPDPPSO; así como en los Lineamientos Generales; las Políticas de Gestión de Datos Personales del Instituto Mexicano de la Radio y demás normatividad aplicable en la materia.

Dicho monitoreo, permitirá verificar que los parámetros establecidos en la LGPDPPSO, en los Lineamientos Generales se cumplan cabalmente o permitan realizar los ajustes necesarios para su cumplimiento.

La finalidad de la implementación de este monitoreo permitirá garantizar el tratamiento óptimo de los datos personales en posesión del IMER, y así determinar las medidas preventivas y/o correctivas a seguir, para mejorar los mecanismos, términos y procedimientos en la materia de que se trate.

Para ello, la Unidad de Transparencia en coordinación con las personas servidoras públicas que realizan entre sus funciones tratamientos de datos personales, serán los encargados de ejecutar el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales.

Monitoreo y supervisión periódica de las medidas de seguridad implementadas a los sistemas de datos personales del IMER

Unidad administrativa:	
Sistema de datos personales:	

Tipo de medida de seguridad	Descripción de la medida de seguridad	Monitoreo	Tiempo para la revisión	Resultado del monitoreo
Físicas				
Administrativas				
Técnicas				

Medidas de seguridad físicas:

a) Se deberá prevenir el acceso no autorizado al perímetro de la unidad administrativa, sus instalaciones físicas, áreas críticas, recursos e información;

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

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

d) Se deberá proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

Medidas de seguridad técnicas:

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

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

d) Se deberán gestionar adecuadamente las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

Medidas de seguridad administrativas:

a) Se garantizará por la persona usuaria el deber de confidencialidad respecto de los datos personales que se encuentren bajo su custodia o a los que tenga acceso o conocimiento con motivo de su empleo, cargo o comisión y no se comunique a quien no está legalmente autorizado, incluso después de que finalice la relación laboral con el Instituto.

b) Se deberá resguardar en todo momento cualquier documento que contenga datos personales para evitar que terceros no autorizados tengan acceso a los mismos;

c) No se debe reutilizar hojas que contengan datos personales;

d) No utilizar ningún medio como, celulares, cámaras fotográficas o cualquier otro dispositivo de uso personal, para captar, reproducir o difundir datos personales;

e) Solo el personal autorizado podrá acceder a documentos que contengan datos personales;

f) Se deberá registrar quién accede a los archivos bajo la custodia de cualquier persona servidora pública;

g) Se puede bloquear el equipo cuando la persona servidora pública se ausente y apagarlo al concluir la jornada laboral.

h) Se deberán retirar los documentos que contengan datos personales de: impresora, escáner y fotocopiadora;

i) Se deben resguardar bajo llave documentos o dispositivos que contengan datos personales;

j) Se pueden generar contraseñas complejas con letras y números, mantenerlas en secreto, por el usuario de datos personales;

k) Se debe evita llevar fuera del lugar de trabajo datos personales en dispositivos electrónicos o papel, si es necesario, proteger esa información con una contraseña o sobre debidamente cerrado;

l) Se debe tener cuidado de no dejar dispositivos móviles o portátiles que contengan datos personales desatendido en un lugar público; si es necesario separarse del dispositivo se deberá bloquear tal y como se hace con el equipo del área.

m) Se deberá cumplir con las medidas de seguridad y normas internas;

n) Se deberá comunicar con la persona superior inmediata cualquier incidencia que se detecte en el tratamiento de datos personales;

o) Cuando sea necesario remitir datos personales a otras áreas del Instituto, se deberá comunicar por escrito que son parte de un sistema de protección de datos personales, especificando para qué finalidades pueden tratarlos y la obligación que se tiene de guardar confidencialidad respecto de los mismos.

Durante el Monitoreo y supervisión periódica de las medidas de seguridad implementadas a los sistemas de datos personales del IMER, las unidades administrativas y servidores públicos involucrados, en todo momento deberán:

a. Proporcionar y mantener a disposición del personal autorizado la información, documentación o datos relacionados con el tratamiento de datos personales objeto del monitoreo;

b. Permitir y facilitar al personal autorizado el acceso a archiveros, registros, archivos, sistemas, equipos de cómputo, discos o cualquier otro medio o sistema de tratamiento de los datos personales objeto del monitoreo;

c. Permitir el acceso al personal autorizado al lugar, a las oficinas o instalaciones de las Unidades Administrativas del IMER donde se lleve a cabo el tratamiento de datos personales;

d. Asistir a las reuniones que se programen para los efectos del Monitoreo y supervisión periódica de las medidas de seguridad implementadas a los sistemas de datos personales del IMER, y:

e. Desahogar los requerimientos realizados por el personal autorizado en los plazos y términos que fije.

En razón de lo anterior, el Comité de Transparencia establecerá un plazo límite para que se corrijan las inconformidades detectadas, situación que deberá quedar debidamente documentada.

Acto seguido, se deberá informar al Comité de Transparencia por parte de las unidades administrativas monitoreadas, sobre la implementación de las recomendaciones emitidas en los plazos que se fijen para tal efecto.