DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DEL IMER

CONTENIDO

INTRODUCCIÓN ..... PÁG. 3

OBJETIVO ..... PÁG. 4

GLOSARIO ..... PÁG. 4-7

MARCO NORMATIVO ..... PÁG. 7

ÁMBITO DE APLICACIÓN ..... PÁG. 7-8

SISTEMAS DE DATOS PERSONALES POR UNIDAD ADMINISTRATIVA Y SUS ANEXOS (I, II, III, IV, V, VI, VII, VIII) ..... PÁG. 8-9

INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO (ANEXO A) ..... PÁG. 9

GUÍA DE ROLES Y FUNCIONES PARA LAS PERSONAS QUE TRATAN DATOS PERSONALES EN EL IMER (ANEXO B) ..... PÁG. 10

ANÁLISIS DE RIESGOS (ANEXO C) ..... PÁG. 11

ANÁLISIS DE BRECHA (ANEXO C) ..... PÁG. 11

PLAN DE TRABAJO (ANEXO C) ..... PÁG. 11

MONITOREO Y SUPERVISIÓN DE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS (ANEXO D) ..... PÁG. 12

PROGRAMA GENERAL DE CAPACITACIÓN (ANEXO E) ..... PÁG. 12

INTRODUCCIÓN

La Constitución Política de los Estados Unidos Mexicanos en los artículos 6 y 16 incorpora el derecho de toda persona a la protección de sus datos personales, así como al acceso, rectificación, cancelación y oposición. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO o Ley General) establece por su parte un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados.

Como parte de las disposiciones establecidas en un principio por la Ley Federal de Transparencia Pública Gubernamental (2002) y con el fin de resguardar los datos personales en posesión del Instituto Mexicano de la Radio (IMER), en el año 2006 se elaboró la primera versión del Documento de seguridad. En 2009 se actualizó dicho documento. Por lo que, para la consecución de su objeto, el Instituto cuenta con diversas atribuciones, en cuyo ejercicio tiene acceso al tratamiento de diversos datos personales, los cuales se distribuyen en sus respectivos sistemas de tratamientos.

De acuerdo con la publicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO, 2017), y lo establecido en su artículo 35, el IMER actualiza su Documento de seguridad para la protección de datos personales con el fin de garantizar las medidas de seguridad administrativas, físicas y técnicas señaladas en el artículo 31, 32, 33, 34 y 34 de la LGPDPPSO.

Por lo anterior y para establecer, así como mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, el Instituto Mexicano de la Radio emite el presente documento, en observancia de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, con la intención de brindar homogeneidad en la organización y procesos para la protección de los mismos.

El presente Documento de seguridad contiene las medidas de seguridad administrativas, físicas y técnicas aplicables a los sistemas de tratamiento de datos personales del IMER, las cuales aseguran la integridad, confidencialidad y disponibilidad de la información que éstos contienen.

Su propósito es identificar los sistemas de tratamiento de datos personales que poseen las unidades administrativas, el tipo de datos personales que contiene cada una de ellas, los responsables, encargados, usuarios de cada sistema y las medidas de seguridad implementadas en los mismos.

Asimismo, el presente documento tiene como propósito controlar internamente el universo de datos personales en posesión del Instituto, el tipo de datos personales que contienen los archivos, los responsables, las obligaciones, el análisis de riesgos, el análisis de brecha, plan de trabajo y los mecanismos de monitoreo y la revisión de las medidas de seguridad, entre otros.

OBJETIVO

El presente Documento de seguridad tiene como objetivo describir las medidas de seguridad de los sistemas de datos personales que maneja el IMER, desde su obtención, almacenamiento, uso, utilización, divulgación, bloqueo y supresión. Asimismo, documentar los aspectos administrativos relativos con la gestión de incidencias, procedimientos de obtención de copias de seguridad, así como establecer las responsabilidades del personal en relación con la protección de los datos personales.

GLOSARIO

Activo: En términos generales, un activo es cualquier elemento que represente un valor para la organización. Según la Real Academia Española, «valor» se define como: a) grado de utilidad o aptitud de las cosas para satisfacer las necesidades o proporcionar bienestar o deleite, y b) cualidad de las cosas, en virtud de la cual se da por poseerlas cierta suma de dinero o equivalente.

Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.

Amenaza: Son los eventos que pueden desencadenar un incidente.

Aviso de privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, 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 referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Borrado seguro: Es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales, de modo que la probabilidad de recuperarlos sea mínima.

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.

Consejo Nacional: Consejo Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refiere el artículo 32 de la Ley General de Transparencia y Acceso a la Información Pública.

Ciclo de vida. Se refiere a las fases de tratamiento de los datos personales, consistentes en la obtención, almacenamiento, uso, divulgación, bloqueo y cancelación.

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

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, información biométrica, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información como puede ser nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social de la persona;

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

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

Encargado: La 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.

Exposición al riesgo: Es la exposición de un activo (datos personales) ante una amenaza cuando se materialice.

Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable.

Garantía de la Seguridad de la información: Es la implementación de Medidas Administrativas, Físicas y Técnicas eficaces para garantizar y velar por la Integridad, Confidencialidad y Disponibilidad de tus datos personales.

Impacto: Es la consecuencia de materialización de una amenaza.

Inventario de Datos Personales: Identificación de las bases de datos de tratamiento de las Unidades Administrativas, por el cual se documenta la información básica de cada tratamiento realizado, con independencia de su forma de almacenamiento, entre lo cual se incluye el ciclo de vida del dato personal.

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

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

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de datos personales.

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.

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.

Órgano garante: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Portabilidad de datos personales: Prerrogativa de los titulares de datos personales que les permite, bajo las condiciones establecidas en la normatividad aplicable, recibir los datos personales que han proporcionado a un responsable del tratamiento en un formato estructurado de uso común y lectura mecánica y trasmitirlos a otro responsable del tratamiento sin impedimentos.

Principios. El derecho a la protección de los datos personales se regula a través de ocho principios, los cuales se traducen en obligaciones, estos son: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

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

Responsable: Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales.

Riesgo: Contingencia o proximidad de un daño.

Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Titular de la unidad administrativa. Persona responsable del tratamiento de los datos personales en la Unidad Administrativa a su cargo.

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

Transferencia: 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 sobre datos personales o conjunto de datos personales, mediante procedimientos manuales o automatizados relacionadas con la obtención, uso, registro, organización, estructuración, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión o cualquier otra forma de habilitación de acceso, cotejo, interconexión, manejo, aprovechamiento, divulgación, transferencia, supresión, destrucción o disposición de datos personales.

Usuario: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

Vulneración: Son las debilidades que tienen los activos ante las amenazas.

Vulneraciones: La pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada.

MARCO NORMATIVO

- Constitución Política de los Estados Unidos Mexicanos (artículos 6 y 16).
- Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.
- Ley General de Transparencia y Acceso a la Información Pública
- Ley Federal de Transparencia y Acceso a la Información Pública
- Lineamientos Generales de Protección de Datos Personales para el sector
- Decreto de creación del IMER (última actualización 18/12/2020)
- Estatuto Orgánico del Instituto Mexicano de la Radio.

ÁMBITO DE APLICACIÓN

En atención a los Deberes referidos en la LGPDPPSO, el presente documento es aplicable para todas las unidades administrativas del IMER que, en el ejercicio de sus atribuciones y funciones traten datos personales, administren bases de datos en sistemas de tratamiento, ya sea que administren sistemas completos, o una parte de la información que le corresponda.

Asimismo, serán aplicables al tratamiento de datos personales que obren en soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación,

procesamiento, almacenamiento y organización. Los datos personales podrán ser expresados en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o en cualquier otro formato.

Todos los servidores públicos que tengan acceso a los datos personales están obligados a conocer y aplicar las medidas de seguridad propias de cada Sistema en el que se concentren los datos y es aplicable en todas y cada una de las fases del tratamiento de los datos personales, desde la obtención de los mismos y finalizando con su eliminación. Cabe mencionar que, la obligación de confidencialidad, debe subsistir aún después de que los involucrados hayan finalizado su participación en el tratamiento de los datos personales porque hayan cambiado de funciones y aun cuando la relación laboral con el IMER haya concluido.

SISTEMAS DE DATOS PERSONALES DEL IMER POR UNIDAD ADMINISTRATIVA

Dirección de Producción y Programación

1. Contratación prestadores de servicios profesionales independientes
2. Convenio de colaboración y/o contratos
3. Base de datos SIC, ingesta de información para reportes
4. Préstamo de documento sonoro

Dirección de Radiodifusoras

1. Carpeta de ganadores
2. Visitas guiadas
3. Contratación prestadores de servicios profesionales independientes

Dirección del Sistema Nacional de Noticiarios

1. Contratación prestadores de servicios profesionales independientes
2. Recopilación de datos personales y de contacto de colaboradores del Sistema Nacional de Noticiarios

Dirección de Administración y Finanzas

1. Contratación al personal de nuevo ingreso y actualización de expediente personal
2. Ingreso de prestadores de servicio social y/o prácticas profesionales
3. Contratación de personas prestadoras de servicios free-lance
4. Pago a proveedores y a prestadores de servicios por honorarios profesionales
5. Contrataciones de personas prestadoras de servicios profesionales independientes

Dirección de Investigación

1. Sistema de solicitudes de acceso a la información y derechos ARCO
2. Manejo y envío de formato de llamadas para las emisoras del IMER
3. Contrataciones de personas prestadoras de servicios profesionales independientes
4. Mecanismos de participación ciudadana

Dirección de Ingeniería

1. Contratación prestadores de servicios profesionales independientes

Dirección de Comercialización y Mercadotecnia

1. Contratación de Servicios
2. Venta de servicios (ingeniería, producción y transmisión directa)
3. Apoyo Social
4. Contrataciones de personas prestadoras de servicios profesionales independientes

Unidad Jurídica

1. Elaboración y validación de instrumentos jurídicos
2. Contratación prestadores de servicios profesionales independientes

INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO (ANEXO A)

Con relación a lo previsto en el artículo 33, fracción III de la Ley General, el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:

I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;

II. Las finalidades de cada tratamiento de datos personales;

III. El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;

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

V. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;

VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y

VII. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

VIII. Ciclo de vida de los datos personales en el inventario de éstos

Aunado a lo dispuesto en el artículo anterior de los presentes Lineamientos generales, en la elaboración del inventario de datos personales el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:

I. La obtención de los datos personales;

II. El almacenamiento de los datos personales;

III. El 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;

IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;

V. El bloqueo de los datos personales, en su caso, y

VI. La cancelación, supresión o destrucción de los datos personales.

GUÍA DE ROLES Y FUNCIONES PARA LAS PERSONAS QUE TRATAN DATOS PERSONALES EN EL IMER (ANEXO B)

Los presente guía tiene como propósito orientar sobre la asignación de roles y funciones de los servidores públicos que participen en alguno de los procedimientos de los sistemas de datos personales con los que cuenta el Instituto Mexicano de la Radio, de acuerdo con lo establecido en el artículo 33, fracción II y 35, fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como lo señalado en el artículo 57 de los lineamientos generales en la materia.

Para realizar un desempeño adecuado en el tratamiento de los datos personales y de los sistemas de datos personales institucionales, se deberán considerar y asignar, de acuerdo con los requerimientos de cada unidad administrativa, las siguientes figuras en el tratamiento de datos personales: Propietario del sistema, Administrador, Usuarios y Custodios.

Por lo anterior, las funciones del servidor público encargado de tratar datos personales y sus tareas específicas, así como la cadena de rendición de cuentas de todas las personas que participen en alguno de los procesos, quedan establecidas en esta guía para que los propietarios de los sistemas de datos personales designen el rol y funciones de las personas participantes en alguna de las tareas o procesos a realizar en materia de protección de datos personales.

ANÁLISIS DE RIESGOS (ANEXO C)

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 (ANEXO C)

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 (ANEXO C)

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.

MONITOREO Y SUPERVISIÓN DE LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS (ANEXO D)

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, interna y/o externa, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

PROGRAMA GENERAL DE CAPACITACIÓN (ANEXO E)

Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.

En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente artículo, el responsable deberá tomar en cuenta lo siguiente:

I. Los requerimientos y actualizaciones del sistema de gestión;

II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;

III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y

IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.