GOBIERNO MUNICIPAL
MONTEMORELOS, NUEVO LEÓN

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES DE LA ADMINISTRACIÓN PÚBLICA MUNICIPAL DE MONTEMORELOS, N.L. 20

INTRODUCCIÓN

En la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León se establecen las bases, principios, procedimientos y tratamiento que permite garantizar la protección de datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los ciudadanos en posesión de la Administración Pública Municipal del Municipio de Montemorelos, como sujetos obligados, teniendo como base dicha normatividad, y el cumplimiento de lo establecido en el artículo 41 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, se crea el presente documento de seguridad.

Dicho numeral señala que el documento de seguridad deberá contener por lo menos el inventario de datos personales y de los sistemas de tratamiento; las funciones y obligaciones de las personas que traten datos personales; el análisis de riesgo; el análisis de brecha, el plan de trabajo; los mecanismos de monitoreo y revisión de las medidas de seguridad; y el programa general de capacitación.

En ese sentido, la Contraloría Municipal de Montemorelos, a través de la Unidad de Transparencia, en conjunto con los enlaces de transparencia que tiene en cada área generadora de información, ha realizado acciones y actividades que tuvieron como finalidad establecer los principios para la creación de este documento.

Para recabar información precisa, se realizaron auditorías a diferentes Unidades Administrativas de la Administración Pública Municipal del Municipio de Montemorelos, con la finalidad de detectar medidas de seguridad con las que ya contaba cada área y dependencia, analizar las brechas de seguridad y definir posibles riesgos.

Una vez emitido el dictamen se generaron cada una de las partes que integran el presente documento de seguridad, siguiendo como objetivo el propiciar la protección de los datos personales de la forma más completa, ello encaminado a lograr el adecuado tratamiento de los datos personales y su protección.

MARCO NORMATIVO

CONSTITUCIÓN POLÍTICA DEL ESTADO LIBRE Y SOBERANO DE NUEVO LEÓN

Artículo 10.- Todas las personas tienen derecho al acceso a la información pública, veraz y oportuna, y a la protección de los datos personales.

Artículo 13.- Las personas tienen derecho a la protección a la vida privada, incluyendo la Información personal que se encuentre en las tecnologías de la información y comunicación. Los sujetos obligados, en términos de la legislación general aplicable, deberán proteger los datos personales en posesión de las autoridades.

El Estado promoverá la protección y desarrollo de los derechos y las libertades reconocidos en esta Constitución dentro del ámbito digital y serán plenamente aplicables en ese ámbito. Se promoverá, a través de políticas públicas, la inclusión de todas las personas de la entidad para el ejercicio de sus derechos de forma digital, de manera que se procure el bien común y el fortalecimiento de la comunidad.

LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE NUEVO LEÓN

Artículo 3. Para los efectos de la presente Ley se entenderá por:
...

XV. Documento de seguridad: 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;
...

Artículo 41. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad; y
VII. El programa general de capacitación.

Artículo 54. Con relación a lo previsto en el numeral 38, fracción III, de la Ley, 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 formato 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.

Artículo 56. Para dar cumplimiento al artículo 38, fracción IV, de la Ley, 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 37 de la ley de protección de datos personales en posesión de sujetos obligados del Estado de Nuevo León.

Artículo 57. Con relación al artículo 38, fracción V, de la Ley, para la realización de análisis de brecha, el responsable deberá considerar la 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 reemplazar a uno o más controles implementados actualmente.

Artículo 58. De conformidad con lo dispuesto en el artículo 38, fracción VI, de la Ley, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y 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 nueva o faltante.

Artículo 59. Con relación al artículo 38, fracción VII, de la Ley, 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 aquellas 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.

Artículo 60. Para el cumplimiento de lo previsto en el artículo 38, fracción VIII, de la Ley, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tenga 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 de sistemas 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 de 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.

GLOSARIO

- **ACTIVO.-** Es la información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para el responsable.
- **BASES DE DATOS.-** Es el conjunto ordenado de datos personales referentes a una persona física identificada condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
- **CONFIDENCIALIDAD.-** Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no automatizados;
- **INSTITUTO ESTATAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE NUEVO LEÓN (INFONL).-** Es un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, conformado por ciudadanos designados por el Poder Legislativo, con plena autonomía técnica, de gestión, de capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.
- **DERECHOS ARCO.-** Los derechos de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales.
- **DISOCIACIÓN.-** Es el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, debido a su estructura, el contenido o grado de desagregación, la identificación del mismo.
- **DISPONIBILIDAD.-** Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados:
- **DOCUMENTO DE SEGURIDAD.-** 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.
- **UT.-** Unidad de Transparencia de la Contraloría Municipal de Montemorelos, N.L.
- **ENCARGADO.-** Persona físico o jurídico, público o privado, ajeno a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por

cuenta del responsable.

- **EVALUACIÓN DE IMPACTO EN LA PROTECCIÓN DE DATOS PERSONALES.-** Es el documento mediante el cual se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones.
- **HARDWARE.-** Es el conjunto de componentes físicos de los que está hecho el equipo.
- **INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES (INAI).-** Es el organismo constitucional autónomo garante del cumplimiento de dos derechos fundamentales: el acceso a la información pública y el de protección de datos personales.
- **INTEGRIDAD.-** La propiedad de salvaguardar la exactitud y completitud de los activos.
- **INVENTARIO DE DATOS PERSONALES.-** Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de la Administración Pública Municipal, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.
- **LEY.-** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León
- **LINEAMIENTOS.-** Lineamientos de Protección de Datos Personales para los Sujetos Obligados del Estado de Nuevo León.
- **MEDIDAS DE SEGURIDAD.-** Es el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales.
- **MEDIDAS DE SEGURIDAD ADMINISTRATIVAS.-** Son la 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, formación 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.-** Son el 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 recursos involucrados en su tratamiento.
- **N/A.-** No aplica.
- **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.
- **RED DE ÁREA LOCAL (LAN).-** Es una red de computadoras que abarca un área reducida a una casa, departamento o edificio.
- **RESPALDO.-** Es una copia de la información que se genera, utiliza y actualiza a lo largo del tiempo; también este término se emplea para referirse a las copias de seguridad que se llevan a cabo en los sistemas de información, bases de datos, software de aplicación, sistemas operativos, utilerías, entre otros. El objetivo de un respaldo es garantizar la recuperación de la información, en caso de que haya sido eliminada, dañada o alterada

al presentarse alguna contingencia.

- **RESPONSABLE.-** Lo es el Municipio de Montemorelos, al ser quien determina los fines, medios, alcance y demás cuestiones relacionadas con el tratamiento de los datos personales.
- **RIESGO.-** Es la combinación de la probabilidad de un evento y su consecuencia desfavorable.
- **RIESGO DE SEGURIDAD.-** Es la probabilidad de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio del Municipio de Montemorelos.
- **SEGURIDAD DE LA INFORMACIÓN.-** Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.
- **SUPRESIÓN.-** Es 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 establecidas por el responsable.
- **TITULAR.-** Es la persona física a quien pertenecen los datos personales.
- **TRANSFERENCIA.-** Es toda comunicación de datos personales fuera del Sujeto Obligado (Municipio de Montemorelos), realizada a persona distinta del titular, responsable o encargado.
- **TRATAMIENTO.-** Es cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionado esto con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.
- **SOFTWARE.-** Es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo.
- **UNIDAD ADMINISTRATIVA.-** Aquella(s) que se encuentra(n) subordinada(s) jerárquica y funcionalmente a las Dependencias señaladas en el artículo 18 del Reglamento Orgánico del Gobierno Municipal de Montemorelos, Nuevo León; integrada por recursos humanos, materiales, financieros y demás archivos físicos y electrónicos, dentro de la administración pública Municipal.
- **ZONA DESMILITARIZADA (DMZ).-** También conocida en seguridad informática como red perimetral, siendo una zona insegura que se ubica entre la red interna de una organización responsable y una red externa, generalmente el internet, teniendo como objetivo, que las conexiones desde la red interna y externa de la DMZ estén permitidas, mientras que en general las conexiones desde la DMZ sólo permitan a la red externa, los equipos (host) en la DMZ no pueden conectar red interna, permitiendo que estos equipos externos protejan la red interna en caso de que intrusos comprometan la seguridad de los equipos situados en la zona desmilitarizada.

INVENTARIOS DE DATOS PERSONALES

Se entiende por "inventario de datos personales" al control de documentos y tratamiento de datos personales que realizan las unidades administrativas de la Administración Pública

Municipal del Municipio de Montemorelos, que se encuentran almacenados tanto física como electrónicamente.

Dichos tratamientos de datos personales, se presentan por unidades administrativas previstas en base a la estructura orgánica y el Reglamento Orgánico del Gobierno Municipal de Montemorelos, Nuevo León y la normativa que lo rige, mismas que cuentan o pueden contar, dar tratamiento y, ser responsables o encargados de los datos personales.

Lo anterior, tiene sustento en los artículos 38 fracción III y 41 fracción 1, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, pues disponen la obligación de los responsables de que cuenten con el inventario de datos personales y que este sea parte de las medidas de seguridad implementadas y del documento respectivo, lo anterior con el fin de tener en cuenta el volumen de datos que se tratan al interior de la organización responsable.

DESCRIPCIÓN Y ESTRUCTURA DE LAS BASES DE DATOS DE TRATAMIENTO DE DATOS PERSONALES

En la descripción de cada base de tratamiento de datos personales, se indica cuáles son los datos personales que se recaban, con qué finalidad se obtienen así como su forma de obtención, el fundamento legal que faculta al área administrativa para el tratamiento de dichos datos personales, los medios de almacenamiento, sitios de resguardo, si existe un encargado que actúe a cuenta y nombre de la Unidad Administrativa y la persona servidora pública encargada de administrar la base o inventario de datos personales así como los subordinados que tienen acceso a las mismas.

Es importante destacar que en los inventarios de datos personales se define la "categoría de los datos personales", estableciendo los tipos de datos personales que pueden estar sujetos a tratamiento de acuerdo a las atribuciones de cada unidad administrativa:

- **Datos de identificación y contacto.-** Nombre, genero, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales, identificación personal, imagen.
- **Datos sobre características físicas.-** Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, cicatrices, tatuajes.
- **Datos biométricos.-** Huella dactilar.
- **Datos laborales.-** Puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección y contratación y experiencia/capacitación laboral.
- **Datos académicos.-** Trayectoria educativa, escolaridad, titulo, cédula profesional, certificados y reconocimientos.
- **Datos patrimoniales y/o financieros.-** Bienes muebles, bienes inmuebles, ingresos,

egresas y cuentas bancarias, información fiscal, historial crediticio, número de tarjeta, seguros, afores.

- **Datos legales.-** Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros).
- **Datos relativos a la salud.-** Estado de salud físico presente pasado o futuro, diagnostico, estado de salud mental, información genérica.
- **Datos personales de naturaleza pública.-** Datos que por mandato legal son de acceso público.
- **Datos sobre pasatiempos, entretenimiento y diversión.-** Pasatiempos, aficiones, deportes, juegos de interés.

En el caso de la sección de "forma de obtención directa / indirectamente del titular medios físicos / electrónicos", de la referida tabla, a continuación, se describen el tipo de personas de quienes se obtienen y cómo se recaban datos personales que pueden estar sujetos a tratamiento de acuerdo a las atribuciones de cada unidad administrativa:

- Personas que laboran en las Direcciones de cada dependencia y entidad de la Administración Pública Municipal.
- Personas externas que prestan algún servicio para las Direcciones de cada dependencia y entidad de la Administración Pública Municipal.
- Personas externas que participan en actividades que llevan a cabo las direcciones de la Administración Pública Municipal de Pesquería, incluyendo (capacitaciones y concursos).

De igual manera se describen las finalidades de cada uno de los tratamientos, el fundamento legal que faculta al área para tratar los datos personales, los formatos en los que se encuentra la información, así como los medios de almacenamiento, por lo que a fin de exponer primeramente los tratamientos que se llevan a cabo al interior se enlistan a continuación.

CATÁLOGO DE TRATAMIENTO DE DATOS PERSONALES

Administración Pública del Municipio de Montemorelos.

Contraloría Municipal	CAPACITACION PRESENCIAL
Contraloría Municipal	DENUNCIAS CONTRA SERVIDORES PÚBLICOS DEL MUNICIPIO DE MONTEMORELOS (OIC)
Contraloría Municipal	RECEPCION Y ATENCIÓN DE DUDAS Y QUEJAS DE LA CIUDADANÍA EN LOS BUZONES DE TRANSAPRENCIA

Contraloría Municipal	SOLICITUDES DE ACCESO A LA INFORMACION PRESENTADA MEDIANTE MODALIDAD DIVERSA A LA PLATAFORMA NACIONAL DE TRANSPARENCIA-PNT
Contraloría Municipal	SOLICITUDES DE EJERCICIO DE DERECHOS ARCO - ACCESO, RECTIFICACION, CANCELACION Y OPOSICIÓN
Contraloría Municipal	SUBSTANCIACIÓN Y RESOLUCION DE PROCEDIMIENTOS DE RESPONSABILIDAD ADMINISTRATIVA
Secretaría de Desarrollo Económico y Fomento Agropecuario	INSCRIPCIÓN A LOS SIGUIENTES PROGRAMAS: "BARRIDO", "A-CERCATE", "JÓVENES AL EMPLEO", "JÓVENES CONSTRUYENDO EL FUTURO", E "IMPULSO".
Secretaría de Desarrollo Económico y Fomento Agropecuario	INSCRICPIÓN A LA BOLSA DE EMPLEO.
Secretaría de Desarrollo Económico y Fomento Agropecuario	LEVANTAMIENTO DE CENSO ECONÓMICO MUNICIPAL.
Secretaría de Desarrollo Económico y Fomento Agropecuario	SOLICITUDES PARA: RECLUTAMIENTO EN REDES SOCIALES ELECTRÓNICAS, RECLUTAMIENTO INSITU Y AL MÓDULO OFICIALÍA DE PARTES.
Secretaría Ejecutiva	GESTORÍA
Secretaría Ejecutiva	LLAMADA TELEFÓNICA "ESTAMOS CONTIGO"
Desarrollo Integral de la Familia (DIF)	API: CONSULTORIO MÉDICO, DEFENSORÍA MUNICIPAL, TRABAJO SOCIAL, PRIMER CONTACTO PARA BRINDAR ASESORÍA JURÍDICA Y DEPARTAMENTO DE PSICOLOGÍA.
Desarrollo Integral de la Familia (DIF)	ÁREA DE ALIMENTACIÓN ESCOLAR.
Secretaría de Seguridad Pública, Tránsito y Vialidad	DETENCIÓN ADMINISTRATIVA

LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATAN DATOS PERSONALES

Para la aplicación correcta de este documento, es necesario establecer los deberes de las personas servidoras públicas de las Unidades Administrativas de cada dependencia y entidad de la Administración Pública Municipal, que participan en el tratamiento de los datos personales derivado de sus atribuciones.

Los servidores públicos involucrados deberán:

1. Tener a la vista el Aviso de Privacidad.
2. Dar a conocer el aviso de privacidad al titular de los datos personales previo a la obtención de sus datos.
3. En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.
4. Al obtener los datos personales cerciorarse de que la información esté completa, actualizada, veraz y comprensible.
5. Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.
6. Recabar los datos personales para la finalidad para la cual, estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.
7. Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Montemorelos, Nuevo León.
8. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
9. Tomar por lo menos una vez al trienio, un curso, taller o capacitación sobre el tratamiento de datos personales.
10. Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.
11. Tratar los datos personales de manera licita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Nuevo León.

Son obligaciones de los Responsables de las Unidades de Transparencia en relación al tratamiento de datos personales, las previstas en el artículo 99 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León:

I. Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;
II. Gestionar las solicitudes para el ejercicio de los derechos ARCO;
III. Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;

IV. Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envió de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;
V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, y
VII. Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.

Son obligaciones del Comité de Transparencia en relación al tratamiento de datos personales, previstas en el artículo 98 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León:

I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia, en coordinación con el oficial de protección de datos personales, en su caso;
II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;
IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;
V. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad:
VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por la Comisión;
VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales; y
VIII. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

ANALISIS DE RIESGOS

El análisis de riesgo tiene como objetivo alinear la protección de los datos personales que se traten en el Municipio de Montemorelos, con la evolución de las actividades que se

realizan en el mismo, que son cada vez con mayor complejidad, pues para anticiparse y prepararse para los nuevos retos que se suscitan día con día, lo recomendable es tener una responsabilidad proactiva ante el tratamiento de los datos personales gestionando los riesgos y el impacto que estos podrían generar.

En ese sentido, la gestión de riesgos, consiste en implementar un conjunto de acciones definidas con el propósito de controlar la probabilidad de consecuencias o impactos que una actividad puede tener sobre los datos personales que posee el Municipio de Montemorelos, los cuales han de ser protegidos, pues se pretende garantizar el servicio público que se otorga, por lo que debe de idénticas la naturaleza. Ámbito y fines de los tratamientos de datos personales, para poder detectar los niveles de posible vulnerabilidad de la información.

A fin de precisar la medición del nivel de impacto que pudieran tener las vulneraciones a la seguridad de los datos personales, se realiza la siguiente relación de nivel de impacto con descripción del Impactos:

NIVEL DE IMPACTO	DESCRIPCIÓN DEL IMPACTO AL PRESENTAR VULNERACIÓN A LOS TRATAMIENTOS DE DATOS PERSONALES
MUY SIGNIFICATIVO	Afecta al ejercicio de derechos fundamentales y libertades públicas establecidos en la Constitución, y sus consecuencias son irreversibles. Las consecuencias están relacionadas con categorías especiales de datos o relativos a infracciones penales, y es irreversible. Causa un daño social significativo, como la discriminación, y es irreversible. Afecta a interesados en situación de especial vulnerabilidad, en particular niños, y de forma irreversible. Causa pérdidas morales o materiales significativas e irreversibles.
SIGNIFICATIVO	Los casos anteriores cuando los efectos son reversibles. Pérdida de control del interesado sobre sus datos personales, cuando la extensión de los datos sea alta con relación a las categorías de datos o al número de sujetos. Se produce o puede producirse usurpación de la identidad de los interesados. Pueden producirse pérdidas financieras significativas a los interesados y/o pérdida de confidencialidad de datos sujetos al deber de secreto profesional o vulneración del deber de confidencialidad. Existe un perjuicio social para los interesados o determinados colectivos de interesados.
LIMITADO MUY LIMITADO	Perdida muy limitada del control de algún dato personal y a interesados puntuales, que no sea categoría especial o relativos a infracciones o condenas penales de carácter irreversible. Pérdidas financieras insignificantes e irreversibles y/o Pérdida de confidencialidad de datos sujetos al secreto profesional pero que no sean categorías especiales o sobre infracción penales. En el caso anterior, cuando todos los efectos son reversibles.

Ahora bien, existen probabilidades de vulneraciones de acuerdo a la documentación generada en base a los tratamientos, o bien, las bases de datos con las que se cuente, lo cual puede ser definido como se describe en el siguiente cuadro:

RIESGO DE VULNERACION DE DATOS PERSONALES	DEFINICIÓN
MUY ALTO	Si el factor de riesgo está materializado y no depende de la probabilidad. Si hay constancia de diversas materializaciones de dicho riesgo en el último año en distintas entidades. Si hay constancia de una materialización de dicho riesgo en el último año en la misma entidad. Existen auditorias/estudios que identifican importantes vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo.
ALTO	Cuando se materializó el riesgo en el último año en alguna entidad. Existen estudios que determinan que la probabilidad podría ser alta. Existen auditorias o estudios que identifican posibles vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo. Los elementos vinculados con los factores de riesgo se han implementado con tecnologías o procedimientos organizativos no maduros, sin seguir normas de calidad, sin estar certificados por terceros independientes
BAJA	Antecedente de una materialización de dicho riesgo en los últimos 10 años en alguna entidad.
IMPROBABLE	Cuando no existe evidencia de la materialización de dicho riesgo en ningún caso

Ahora bien, por cada tratamiento de datos personales se solicita diversa información conformando las bases de datos con que se cuenta, por lo que a continuación se presentan los niveles de riesgo de acuerdo al tipo de dato personal que se trata en posesión del Municipio como se refiere a continuación:

TIPO DE DATO O INFORMACIÓN	NIVEL DE RIESGO
Documentos Personales: ➢ Correos electrónicos ➢ Actas de Nacimiento ➢ CURP ➢ RFC ➢ Certificación Única Policial CUP ➢ Clave de elector ➢ Identificaciones ➢ Documentos académicos ➢ Documentos patrimoniales ➢ Firma autógrafa ➢ Entre otros	**MEDIO**
Aspectos personales: ➢ Personas o grupos con los que se relaciona ➢ Roles sociales ➢ Capacidad de adaptación ➢ Tolerancia al riesgo ➢ Gustos/preferencias de contenidos audiovisuales (televisión interactiva, plataformas de contenidos, redes sociales...) ➢ Cuidado de salud ➢ Culturales (lectura, música, arte,...) ➢ Pertenencia y actividades en asociaciones sociales y culturales ➢ Entre otros	**ALTO**
Preferencias de consumo, hábitos, gustos, necesidades, etc. que no permitan inferir informaciones relacionadas con categorías especiales de datos. ➢ Preferencias de consumo: categoría de comercio, tipo de establecimiento; tipo de productos; etc. ➢ Hábitos de consumo ➢ Preferencias de contenidos audiovisuales en diferentes medios (televisión interactiva, plataformas de contenidos, redes sociales, ...) ➢ Preferencias de ocio (deportes, restaurantes, museos, teatros, música, etc.)	**BAJO**

Datos laborales: ➢ Control de acceso al lugar de trabajo; ➢ Número de Seguridad Social ➢ Incidencias ➢ Capacitaciones ➢ Referencias laborales ➢ Referencias personales ➢ Solicitud de empleo ➢ Grabación de imágenes en zonas de acceso o en oficinas; ➢ Títulos ➢ Cédula profesional ➢ Certificados ➢ Reconocimientos ➢ Currículum ➢ Grabación de audio en zonas de acceso o en oficinas; ➢ Monitorización de los equipos de los empleado; ➢ Inferencia del rendimiento a través de indicadores (Productividad y calidad del trabajo, Eficiencia, Formación adquirida, objetivos conseguidos); ➢ Entre otros.	**MEDIO**

Situación económica: ➢ Renta personal ➢ Ingresos mensuales ➢ Patrimonio (bienes muebles/inmuebles) ➢ Situación laboral ➢ Entre otros.	**MEDIO**
Estado financiero: ➢ Solvencia financiera ➢ Pasivos (gastos en alimentación, vivienda, educación, salud, impuestos, pagos de créditos, tarjetas de crédito o gastos personales, etc.; ➢ Nivel de deuda (Préstamos personales, hipotecas) ➢ Ingresos. ➢ Entre otros.	**MUY ALTO**
Información Bancaria: ➢ Cuentas bancarias. ➢ Tarjetas. ➢ Entre otros.	**MUY ALTO**

Datos de comportamiento de empleados: ➢ Fiabilidad de la persona ➢ Hábitos y valores que facilitan la convivencia ➢ Hábitos y valores que facilitan el trabajo y el estudio ➢ Hábitos y valores que influyen en el bienestar personal, laboral y familiar ➢ Hábitos y valores que influyen en el compromiso con las personas y con la sociedad ➢ Estabilidad laboral. ➢ Antecedentes de comportamiento ➢ Entre otra información.	**MEDIO**

Datos de localización: ➢ Registro de desplazamientos ➢ Registro de lugares habituales ➢ Registro de rutinas en base a localización ➢ Registro de lugares habituales	**MEDIO**

Historial de salud ➢ Historial clínico ➢ Informes de salud ➢ Enfermedades ➢ Incapacidad médica ➢ Informes de baja laboral por motivas de salud para el Servicio de Prevención de Riesgos Laborales ➢ Recetas medicas ➢ Datos relativos a salud física ➢ Datos relativos a salud mental ➢ Datos relativos a prestación de servicios de atención sanitaria ➢ Documentos relativos a procesos asistenciales del paciente (incluida identificación de médicos y demás profesionales que han intervenido) ➢ Cualquier información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. ➢ Datos Genéticos	**ALTO**

Datos biométricos: ➢ Huella dactilar ➢ Reconocimiento facial ➢ Iris ➢ Voz ➢ Gestos ➢ Modo de andar ➢ Descriptores corporales de cualquier índole ➢ Trazo (firma)	**ALTO**
Categorías especiales de datos o que permitan inferirlos: ➢ Origen étnico ➢ Origen racial ➢ Opiniones políticas ➢ Convicciones religiosas ➢ Convicciones filosóficas ➢ Afiliación sindical ➢ Datos relativos a la salud ➢ Datos relativos a la vida sexual ➢ Datos relativos a las orientaciones sexuales ➢ Entre otros	**ALTO**

Datos personales relativos a probables delitos e infracciones administrativas.	**MUY ALTO**
Metadatos: ➢ Datos de tratico de las comunicaciones electrónicas ➢ Identificación de emisor y/o receptor en las comunicaciones ➢ Datos en conexiones a internet: localización; características software y hardware del dispositivo con el que se conecta; redes sociales o páginas en general en las que se ha logado, conexión (IP, proveedor de servicios, velocidad de descarga). ➢ Código de barras y digital ➢ Cifrado (número de control óptico) credencial para votar ➢ Número de OCR (reconocimiento óptico de caracteres) credencial para votar parte posterior ➢ Firma electrónica ➢ Entre otros.	**MEDIO**

Datos de Identificación: ➢ Bajo ➢ Nombre ➢ Estado Civil ➢ Fecha de Nacimiento. ➢ Nacionalidad ➢ Lugar de nacimiento ➢ Domicilio ➢ Teléfono ➢ Correo electrónico ➢ Edad ➢ Fotografía ➢ Sexo ➢ QR ➢ Matrícula del servicio militar nacional ➢ Número de pasaporte	**BAJO**

Por lo que toca a los tratamientos relacionados a los menores de edad, personas adultas mayores, personas en situación de vulnerabilidad, victimas discapacitados, etc., se analiza el riesgo de la información personal de acuerdo al siguiente cuadro:

CATEGORIA DE TITULAR / FACTOR DE RIESGO	NIVEL DE RIESGO
Menores de 14 años	Muy Alto
Víctimas de violencia de género	Muy Alto
Menores dependientes de sujetos vulnerables	Muy Alto
Personas bajo guardia y custodia de víctimas de violencia de género	Muy Alto
Mayores con según grado de discapacidad	Muy Alto
Personas con enfermedades mentales	Muy Alto
Discapacitados	Muy Alto
Sujetos en riesgo de exclusión social	Muy Alto
Pacientes	Alto
Personas mayores	Alto
Personas que acceden a servicios sociales	Medio

En este contexto, una vez evaluado el nivel de riesgo de los datos personales que se tratan al interior del Municipio de Montemorelos, se establecerá la probabilidad de que se materialice el impacto de vulnerabilidad con la cantidad de titulares que se establecen en los tratamientos; lo anterior de precisar de acuerdo en la siguiente tabla:

TIPO DE DATO	NIVEL DE RIESGO INHERENTE
Información financiera y Bancaria	Muy Alta
Titulares de alto Riesgo	Muy Alto
Biométricos	Alto
Salud	Alto
Datos sobre la ideología; creencias religiosas, filosóficas o morales; opiniones políticas y afiliación sindical.	Alto
Datos sobre vida sexual	Alto
Datos de origen étnico o racial	Alto
Patrimoniales	Medio
Académicos	Medio
Laborales	Medio
Características físicas	Medio
Pasatiempos, entretenimiento y diversión.	Bajo
Identificación	Bajo

Ahora bien, resulta indispensable para efectos de calcular la probabilidad de riesgo de posibles vulneraciones, establecer los valores aproximados de la cantidad de titulares de los cuales el Municipio de Montemorelos resguarda su información personal, por lo cual se presenta la siguiente tabla, con el objeto de definir las medidas de riesgos inherentes señalados en la tabla que precede, relacionado a la cantidad aproximada de titulares, arrojando así, un nivel de riesgo el cual, cada número y color, indica gradualmente como aumenta el riesgo de ser vulnerada la información:

RIESGO INHERENTE	NIVEL DE RIESGO				
Muy Alto	4	4	5	5	5
Alto	1	2	3	3	3
Medio	1	1	2	3	3
Bajo	1	1	1	1	1
Número de Titulares aproximado	500	5,000	50,000	500,000	+500,000

Nivel de riesgo, expresa la posibilidad de materializarse una vulneración y la afectación que esto generaría, como se describe a continuación:

Riesgo por tipo de dato Nivel 1, ocurre cuando:

1. El nivel de riesgo inherente de los datos sea bajo, sin importar el número de personas.
2. El nivel de riesgo inherente sea medio y se tengan hasta cinco mil (5,000) personas.
3. El nivel de riesgo inherente sea alto y se tengan hasta quinientas (500) personas.

Riesgo por tipo de dato Nivel 2, ocurre cuando:

1. El nivel de riesgo inherente de los datos personales sea medio y se tengan hasta cincuenta mil (50,000) personas.
2. El nivel de riesgo inherente de los datos personales sea alto y se tengan hasta cinco mil (5,000) personas.

Riesgo por tipo de dato Nivel 3, ocurre cuando:

1. El nivel de riesgo inherente de los datos personales sea medio y se tenga de cincuenta mil (50,000) personas en adelante
2. El nivel de riesgo inherente de los datos personales sea alto y se tenga de cinco mil (5,000) personas en adelante.

Riesgo por tipo de dato Nivel 4, ocurre cuando:

1. El nivel de riesgo inherente de los datos personales sea muy alto y se tengan hasta cinco mil (5000) personas.

Riesgo por tipo de dato Nivel 5, ocurre cuando:

1. El nivel de riesgo inherente de los datos personales sea muy alto y se tengan más de cincuenta mil (50,000) personas.

En virtud de las categorías de datos previamente medidas de acuerdo a su naturaleza con el nivel de impacto, se procede a materializar la evaluación del riesgo, de acuerdo al tipo de tratamiento, por el número de titulares, para lo cual, se realiza la siguiente Matriz de Análisis de Riesgo:

ACTIVIDAD O CATEGORIA DE DATOS	NIVEL DE IMPACTO	VULNERABILIDAD	NÚMERO DE TITULARES	NIVEL DE RIESGO
ACTIVIDAD				
Perfilación: ➢ Creación de perfiles ➢ Uso de perfiles ➢ Clasificación de individuos ➢ Orientación de productos/servicios a individuos o grupos ➢ Análisis comportamental (evaluación y calificación de emociones, estados de ánimo, hábitos, preferencias, etc.) Entre otros que pudieran derivar.	Alto	Acceso no autorizado al rastro digital de las y los usuarios, vulnerando a información de acuerdo al comportamiento de que se trate o finalidad de la actividad.	+ 5,000	3
Predicción: ➢ Inferencia de nuevos datos personales. ➢ Modificaciones. Entre otros que pudieran derivar.	Alto	Vulneración de registros de los datos personales de servidores públicos Y usuarios que han otorgado su consentimiento para automatizar sus datos.	+ 500	1
Control de los Servidores Públicos: ➢ Evaluación del empleado ➢ Observación del puesto de trabajo ➢ Monitorización del puesto de trabajo ➢ Grabación de imágenes en ámbito laboral ➢ Grabación de audio en ámbito laboral	Medio	Información de lugar, tiempo y hora donde radican los servidores públicos, así como los cambios de turnos, modo y lugares de vigilancia.	+ 50,000	3

➢ Monitorización por medio de imágenes en ámbito laboral ➢ Monitorización por medio de sonido en ámbito labora ➢ Tiempo invertido en realizar tareas ➢ Monitorización y control de correo electrónico ➢ Control de Asistencia. ➢ Control de uso de teléfono Entre otros que pudieran derivar.				

Control del Acceso a Internet: ➢ Análisis o evaluación de tiempos de uso de internet ➢ Control de permisos para actividades de navegación en Internet ➢ Análisis o evaluación de alarmas sobre navegación ➢ Sitios específicos en Internet ➢ Análisis o evaluación de alarmas sobre navegación a contenidos específicos en Internet Entre otros que pudieran derivar.	Medio	Vulneraciones a las redes internas así como a la información de sitios de navegación de cada servidor, así como las permisos para autorizaciones en la red, lo cual no constituye el ingreso a los servidores donde se almacena información.	+5,000	2
Observación: ➢ Vigilancia mediante imágenes ➢ Vigilancia mediante sonidos ➢ Vigilancia de comunicaciones ➢ Vigilancia de Internet. Entre otros que pudieran derivar.	Alto	Vulneración a la video vigilancia de los edificios y centros físicos del Municipio, así como de las comunicaciones oficiales de Información en la nube.	+ 50,000	3

Monitorización: ➢ Control mediante Imágenes Control mediante sonidos ➢ Control de comunicaciones ➢ Control de transmisiones ➢ Control de internet Entre otros que pudieran derivar.	Alto	Vulneración a los centros de control físicos y virtuales, así como a las redes comunicaciones de datos y la Ubicación de los mismos.	+ 50,000	3
Supervisión: Control ➢ Análisis mediante imágenes ➢ Análisis mediante sonidos ➢ Análisis de comunicaciones ➢ Análisis de transmisiones ➢ Análisis de Internet ➢ Control de tráfico rodado ➢ Entre otros que pudieran derivar.	Alto	Acceso no autorizado a la información relativa a la supervisión de actividades de las y los servidores públicos.	+ 50,000	3

Control físico de acceso: ➢ Control de acceso a las instalaciones ➢ Control de acceso a eventos ➢ Control de acceso a instalaciones deportivas ➢ Control de acceso a las áreas en específico. Entre otros que pudieran derivar.	Bajo	Acceso de personas no autorizadas a la información de quienes accedan a las instalaciones o quienes acuden a los eventos del Municipio, vulnerando su información que les es recabada.	+ 50,000	1
Decisiones automatizadas sin intervención humana.	Alto	No aplica		

Decidir sobre o impedir el ejercicio de derechos fundamentales: ➢ Derecho a la igualdad ➢ Derecho a la no discriminación ➢ Derecho a la vida y a la integridad física ➢ Derecho a la libertad religiosa ➢ Derecho a la libertad personal ➢ Derecho al patrimonio ➢ Derecho a la intimidad personal y familiar ➢ Derecho a la propia imagen ➢ Derecho a la libertad de expresión e información ➢ Derecho a la libertad de cátedra ➢ Derecho a la libertad de reunión ➢ Derecho a la libertad de asociación ➢ Derecho al libre acceso a cargos y funciones públicas en condiciones de ➢ Igualdad ➢ Derecho a la legalidad penal ➢ Derecho a la educación ➢ Derecho a la libertad sindical	Alto	Vulneración a los procesos que se llevan a cabo en el Municipio o sus dependencias, referentes a solicitudes, servicios, procedimientos, dudas o quejas así como cualquiera que se encuentre dentro de las facultades del Municipio de Montemorelos.	+ 500,000	3
➢ Derecho de petición Otros derechos libertades Consagradas en la Constitución Política de los Estados Unidos Mexicanos.				
Decidir sobre el control del interesado de sus datos personales: ➢ Derecho de acceso ➢ Derecho de rectificación ➢ Derecho de oposición ➢ Derecho de Cancelación	Alto	Privar de los derechos de los titulares en materia de protección de datos personales.	+ 500,000	3

➢ Derecho a la portabilidad				
Decidir sobre el acceso a un servicio de los que presta el Municipio de Montemorelos.	Alto	Vulnerar la necesidad de un servicio municipal, de las y los ciudadanos al solicitar un servicio.	+ 500,000	3
Decidir sobre la realización o ejecución de un contrato tanto laboral como de proveedores,	Alto	Riesgo de que no se materialice el trabajo o el servicio por fuga de información.	+ 500	2
Decidir sobre el acceso a servicios financieros de apoyo.	Muy Alto	Afectar a los beneficiarios beneficiarias a un apoyo.	+ 500	3
Servicios o trámites que tengan efectos jurídicos sobre las personas.	Alto	Anticipación a las resoluciones y manipulación o sustracción de Personas No tramites.	+ 50,000	3
Servicios de Salud.	Alto	Vulneración a la intimidad de las Personas y riesgo de Discriminación.	+ 5,000	2
Conservación con fines de archivo	Medio	Vulneración a toda la información o pérdida de la misma en archivos físicos como electrónicos.	+ 500,000	3

DATOS PERSONALES				
Documentos Personales: ➢ Correos electrónicos ➢ Actas de Nacimiento ➢ CURP ➢ RFC ➢ Certificación Única Policial CUP ➢ Clave de elector ➢ Identificaciones ➢ Documentos académicos ➢ Documentos patrimoniales ➢ Firma autógrafa Entre otros	Medio	Vulneración a la información personal de identificación, académica y patrimonial de usuarias y servidores públicos.	+ 500,000	3
Aspectos personales: ➢ Personas o grupos con los que se relaciona ➢ Roles sociales ➢ Capacidad de adaptación ➢ Tolerancia al riesgo ➢ Gustos/preferencias de contenidos audiovisuales(televisión interactiva, plataformas de contenidos, redes sociales,) ➢ Cuidado de salud ➢ Culturales (lectura, música, arte). ➢ Pertenencia y actividades en asociaciones sociales y culturales Entre otros	Alto	Vulneración a los datos que identifican a las personas de acuerdo a sus aspectos personales, pudiendo catalogar a las personas de acuerdo a sus intereses personales.	+ 50,000	3

Preferencias de, consumo, hábitos, gustos, necesidades, etc., que no permitan inferir informaciones relacionadas con categorías especiales de datos: Preferencias de consumo: categoría de comercio, tipo establecimiento; tipo de productos: etc. ➢ Hábitos de consumo ➢ Preferencias de contenidos audiovisuales en diferentes medios (televisión interactiva, plataformas de contenidos, redes sociales). ➢ Preferencias de ocio (deportes, restaurantes, museos, teatros, música, etc.). Entre otros	bajo	Vulneración a los intereses de las personas lo cual pudiera ocasionarles el ser víctimas de fraudes o extorciones, por el conocimiento de sus hábitos, preferencias, gustos, necesidades etc.	+ 500	1
Datos laborales: ➢ Control de acceso al lugar de trabajo; ➢ Número de Seguridad Social ➢ Incidencias ➢ Capacitaciones ➢ Referencias laborales ➢ Referencias personales ➢ Solicitud de empleo ➢ Grabación de imágenes en zonas de acceso o en oficinas; ➢ Títulos ➢ Cédula profesional ➢ Certificados ➢ Reconocimientos ➢ Currículum ➢ Grabación de audio en zonas de acceso o en oficinas; ➢ Monitorización de los equipos de los empleado; ➢ Inferencia del rendimiento a través de indicadores (Productividad y calidad del trabajo, Eficiencia, Formación adquirida, objetivos conseguidos); Entre otros.	Medio	Vulneración al modo de trabajo de as personas, así como a la trabajo.	+ 5,000	2

Situación económica: ➢ Renta personal ➢ Ingresos mensuales ➢ Patrimonio (bienes muebles / inmuebles) ➢ Situación laboral Entre otros.	Medio	Puede ocasionar discriminación, o bien ser objetivos para fraudes o extorciones.	+ 50,000	3
Estado financiero: ➢ Solvencia financiera Pasivos (gastosen alimentación, Vivienda, educación, salud, impuestos, pagos de créditos, tarjetas de crédito o gastos personales, etc; ➢ Nivel de deuda (Préstamos personales, hipotecas) ➢ Ingresos. ➢ Entre otros.	Muy Alto	Puede ocasionar discriminación, o bien ser objetivos para fraudes o extorciones.	+ 5,000	5

Información Bancaria: ➢ Cuentas bancarias. ➢ Tarjetas. Entre otros.	Muy Alto	Puede ocasionar discriminación, o bien ser objetivos para fraudes o extorciones.	+ 5,000	5
De comportamiento de empleados				

➢ Fiabilidad de la persona ➢ Hábitos y valores que facilitan la convivencia ➢ Hábitos y valores que facilitan el trabajo y el estudio ➢ Hábitos y valores que influyen en el bienestar personal, laboral y familiar ➢ Hábitos y valores que incluyen en el compromiso con las personas y con la sociedad ➢ Estabilidad laboral. ➢ Antecedentes de comportamiento. Entre otra información.	Medio	Pueden ser objetos de algún tipo de distinción o de ataques sociales por su comportamiento laboral académico.	+ 5,000	2
Datos de localización: ➢ Registro de desplazamientos ➢ Registro de lugares habituales ➢ Registro de rutinas en base a ➢ localización Registro de lugares habituales	Medio	Puede ser objeto de ataques, fraudes o extorciones el conocer donde se desplazan las y los servidores públicos, los lugares a los que acuden con frecuencia así como sus rutinas y horarios.	+500	1
Datos de Salud: ➢ Historial clínico ➢ Informes de salud ➢ Enfermedades ➢ Incapacidad médica ➢ Informes de baja laboral por motivas de salud para el Servicio de Prevención de Riesgos Laborales ➢ Recetas medicas ➢ Datos relativos a salud física ➢ Datos relativos a salud mental ➢ Datos relativos a prestación de servicios de atención sanitaria ➢ Documentos relativos a procesos asistenciales del paciente (incluida identificación de médicos y demás profesionales que han intervenido) ➢ Cualquier información que se considere trascendental para el	Alto	Pueden ser objeto de ataques a la privacidad personal, discriminación manipulación, o	+ 5,000	3

conocimiento veraz y actualizado del estado de salud del paciente. Datos Genéticos				

Datos biométricos: ➢ Huella dactilar ➢ Reconocimiento facial ➢ Iris ➢ Voz ➢ Gestos ➢ Modo de andar ➢ Descriptores corporales de cualquier ➢ índole Trazos (firma)	Alto	Vulnera los datos de autentificación, lo cual puede traer para las personas perjuicio económico, patrimonial y laboral.	+ 5,000	3
Categorías especiales de dalos o que permitan inferirlos: ➢ Origen étnico ➢ Origen racial ➢ Opiniones políticas ➢ Convicciones religiosas ➢ Convicciones filosóficas ➢ Afiliación sindical ➢ Datos relativos a la salud ➢ Datos de la vida sexual ➢ Datos relativos a las orientaciones ➢ Sexuales Entre otros.	Alto	La vulneración de esta información personal tendría consecuencias morales y sociales ya que pueden ser objeto de discriminación si se difunde esta información o si se tienen accesos no autorizados.	+ 5,000	3

Datos personales relativos probables delitos e infracciones administrativas.	Muy Alto	Puede traer consecuencias de daño moral y físico contra la persona que se encuentre ante un proceso de esta índole	+ 500,000	5

Metadatos: ➢ Datos de tratico de las comunicaciones electrónicas ➢ Identificación de emisor y/o receptor en las comunicaciones ➢ Datos en conexiones a internet: localización; características software y hardware del dispositivo con el que se conecta; redes sociales o páginas en general en las que se ha logado, conexión (IP, proveedor de servicios, velocidad de descarga). ➢ Código de barras y digital ➢ Cifrado (número de control óptico) credencial para votar ➢ Número de OCR (reconocimiento óptico de caracteres) credencial para votar parte posterior ➢ Firma electrónica Entre otros.	Medio	Identificación del movimiento, comunicación y actualización de la información así como de las conexiones de red, lo cual podría poner en riesgo los sistemas internos así como los equipos de cómputo.	+ 5,000	3
Datos de Identificación: ➢ Nombre ➢ Estado Civil ➢ Fecha de Nacimiento. ➢ Nacionalidad ➢ Lugar de nacimiento ➢ Domicilio ➢ Teléfono ➢ Correo electrónico ➢ Edad ➢ Fotografía ➢ Sexo ➢ QR ➢ Matrícula del servicio militar nacional ➢ Número de pasaporte	Bajo	Acceso no autorizado a información del personal del Municipio, o bien a la información de las personas usuarias, vulnerándose su información personal de identificación y contacto.	+ 500,000	1

ANÁLISIS DE BRECHA

Para realizar el análisis de brecha, la Unidad de Transparencia dependiente de la Contraloría Municipal de Montemorelos, realizó una auditoría con el objetivo de efectuar un auto diagnóstico que determine el nivel de desempeño real esperado en cuanto a las medidas de seguridad empleadas por la Administración Pública Municipal.

Una vez identificados los posibles riesgos a los que el Municipio de Montemorelos se encuentra susceptible de enfrentar, se formula el presente análisis de brecha, utilizando como base las siguientes preguntas realizadas durante la auditoría:

1. ¿En qué servicios y trámites específicos de esta Unidad Administrativa se solicita información personal?
2. ¿Conoce la normativa en materia de datos personales?
3. ¿Cuentan con avisos de privacidad integral?
4. ¿Los avisos de privacidad se encuentran en un lugar visible?
5. Conoce el proceso de Acceso, Rectificación, Cancelación, Oposición y Portabilidad de Datos (ARCOP)?
6. ¿Dónde se archivan los documentos que contengan datos personales?
7. ¿La Unidad Administrativa cuenta con un respaldo electrónico de los archivos que contengan datos personales?
8. Las instalaciones, ¿cuentan con medidas de seguridad para el resguardo de los archivos que contienen datos personales?
9. ¿Tienes mecanismos para eliminar de manera segura la información?
10. ¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?

En tal sentido, se tiene que el personal del Municipio de Montemorelos no está familiarizado con la normatividad aplicable en datos personales, no obstante, en cuanto a las actividades tienen claro en cuales servicios y trámites manejan datos personales, derivado del informe de resultados de las auditorías practicadas a las Unidades Administrativas se detecta la necesidad de establecer un plan de trabajo a fin de solventar las observaciones y recomendaciones para mejorar la seguridad de la información personal que se encuentra en los sistemas de tratamiento del Municipio de Montemorelos, motivo por el cual se plantea el siguiente:

PLAN DE TRABAJO

De conformidad con el artículo 38, fracción VI, de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Nuevo León, se presenta el siguiente plan de trabajo del Municipio de Montemorelos, Nuevo León:

Para la ejecución del presente plan de trabajo, se implementará lo siguiente:

a) Aprobación por el Comité de Transparencia del Documento de Seguridad del Municipio de Montemorelos, Nuevo León.

b) Se comunicará a los Titulares de las Unidades Administrativas, enlaces de transparencia para que hagan de conocimiento a todo el personal involucrado en manejo de datos personales sobre la emisión del documento de seguridad y, se dará difusión en versión pública a través de la página oficial del Municipio.

c) Socializar el calendario de capacitaciones en materia de protección de datos personales dirigido a todas y todos los servidores públicos del Municipio de Montemorelos, en los cuales se busque abordar a más personas servidoras públicas para que sean capacitadas, mejorando con esto el conocimiento acerca de los principios y deberes que rigen la materia, así como para crear conciencia de la protección de la información.

Además, dentro del plan de trabajo para tener una mejora en la seguridad de los datos personales que se tratan en el Municipio, se deberán de implementar las siguientes:

MEDIDAS DE SEGURIDAD EN LA ADMINISTRACION PÚBLICA MUNICIPAL DE MONTEMORELOS

Medidas de seguridad físicas y administrativas

Las Dependencias de la Administración Pública Municipal, deberán implementar como mínimo las siguientes medidas generales de seguridad física, para evitar daños, sustracciones o intromisiones no autorizadas en las instalaciones y archivos de información del sujeto obligado:

a) En la medida de lo posible asignar un espacio seguro y adecuado para el tratamiento de datos personales, que no se encuentre a la vista del público y que preferentemente no sea un área de paso frecuente por el personal del trabajo o ajeno al mismo.
b) Tener bajo llave o asegurados los archiveros, archivos, cajas y almacenes en donde se encuentre almacenada la información de datos personales.

c) Evitar que se dejen descuidados o sin la atención debida documentos que contengan datos personales.
d) Establecer un plan de contingencia ante la pérdida total o parcial de datos personales.
e) Verificar que en ningún caso los documentos que contengan datos personales se utilicen como papel reciclable ni de doble uso, ya que una vez transcurridos los plazos en que deban cancelarse o al tratarse de proyectos no utilizables, deberán ser destruidos.
f) Capacitarse en materia de protección de datos personales que permitan la concientización.
g) Elaborar y/o actualizar, cualquiera que sea el caso, los avisos de privacidad, aplicar medidas compensatorias y la puesta de los avisos en lugares visibles dentro de las Unidades Administrativas.

MEDIDAS DE SEGURIDAD DE ARCHIVO

Las medidas de seguridad archivísticas consisten en mecanismos que se valen de la tecnología para respaldar las bases de datos relacionados con datos personales.

Las Dependencias de la Administración Pública Municipal, deberán implementar como mínimo las siguientes medidas, para evitar daños, sustracciones o intromisiones no autorizadas:

- Registrar la información que corresponda en los tratamientos de Datos Personales y mantenerlos actualizados.
- Requerir el apoyo en tecnologías de información para realizar el respaldo correspondiente.
- Verificar que durante los respaldos, mantenimientos, reparaciones y/o monitoreo que el personal interno o externo dé al equipo, no se vulnere la seguridad de la información contenida en su disco duro o cualquiera de sus dispositivos de almacenamiento en la forma que adopten, debiendo estar acompañados por un servidor público autorizado para tal efecto.
- Implementar los demás procedimientos y medidas de seguridad técnicas necesarias para el tratamiento y conservación de datos personales contenidos en sus archivos, registros, bancos y bases de datos, que deriven de lo dispuesto en la Ley de Archivos para el Estado de Nuevo León y la demás normatividad aplicable.

Las Dependencias de la Administración Pública Municipal, implementará cuando menos las siguientes medidas de seguridad en equipos computacionales que contengan documentos, archivos o sistemas de datos personales:

- Limitar o restringir por completo uso de internet en los equipos que se estime pertinente

FORMAS DE ARCHIVO, BAJA Y EXPURGO DOCUMENTAL SEGURO DE INFORMACIÓN, CUYO CONTENIDO SE ENCUENTRAN INMERSOS DATOS PERSONALES

En materia de gestión archivística todos los documentos, expedientes y/o archivos que genere y/o posea el Municipio se deberá colocar un identificador con la leyenda "Contiene datos personales" en su portada en el rubro de observaciones.

Antes de establecer la modalidad de baja y expurgo de los documentos, expedientes y/o archivos que genere y/o posea el Municipio, es indispensable precisar sobre su ciclo de vida, conforme al catálogo de disposición documental que para sus efectos genere o expida el área coordinadora de archivos.

Una vez cumplido el ciclo de vida establecido en el catálogo de disposición documental se procederá al expurgo conforme a la normatividad vigente y protocolos.

Al tratarse de datos personales resguardados físicamente, los riesgos existentes son la pérdida o uso indebido de la información, deterioro negligente, así como su destrucción.

MÉTODOS DE DESTRUCCIÓN

a) Trituración mediante corte cruzado o en partículas, consiste en cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados "partículas", lo cual hace prácticamente imposible que se puedan unir.

b) Destrucción de los medios de almacenamiento electrónicos a través de la desintegración, a fin de que deje de existir la información que se desea eliminar, se separa, completa o parcialmente los elementos que la conforman.

MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Se podrán realizar auditorías ordinarias de acuerdo al Plan Anual, y extraordinarias aleatorias en las Unidades Administrativas para conocer el grado de cumplimiento de las medidas de seguridad.

EL PROGRAMA GENERAL DE CAPACITACIÓN

Nombre:

Plan de Capacitación para los Servidores Públicos del Ayuntamiento de Montemorelos, Nuevo León en Protección de Datos Personales.

Fundamentación:

- Artículo 35, fracción III, 38, fracción VIII, 41, fracción VII, y 98, fracción VII, de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados.
- Artículo 60, de los Lineamientos de Protección de Datos Personales ara los Sujetos obligados del Estado de Nuevo León, emitidos por la Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León ahora INFONL.

Objetivo General:

Que, el Municipio de Montemorelos, Nuevo León, logre incorporar buenas prácticas en el tratamiento de datos personales.

Objetivos específicos:

- Proveer conocimientos y desarrollar habilidades en materia de protección de datos personales y archivo de los mismos.
- Promover mediante el programa de capacitación mejora continua en los procesos que involucren tratamiento de datos personales.
- Contar con avisos de privacidad y medidas compensatorias en cada Unidad Administrativa donde los trámites y servicios involucren datos personales.
- Promover conocimientos para prevenir pérdida total o parcial de datos personales en posesión del sujeto obligado.

Metas:

- Capacitar al 100% de servidores públicos que resguardan información o que tratan datos personales dentro del sujeto obligado.
- Capacitar al 100% de los enlaces de transparencia, encargados de archivo en trámite, grupo multidisciplinario, servidores públicos adscritos a la Unidad de Transparencia y Archivo.

EL PRESENTE DOCUMENTO DE SEGURIDAD FUE ELABORADO EN EL MES DE JUNIO DEL AÑO 2024- DOS MIL VEINTICUATRO Y APROBADO EN LA SESIÓN EXTRAORDINARIA SEXTA DEL COMITÉ DE TRANSAPRENCIA DE FECHA 13-TRECE DE JUNIO DEL PRESENTE AÑO

ELABORÓ	REVISÓ	APROBÓ
Alessandra G		
Lic. Alessandra Mayela Gallardo Zambrano Enlace de Información y Transparencia	C.P. Yajaira Karely Gutiérrez Colunga Contralora Municipal	Comité de Transparencia C.P. Yajaira Karely Gutiérrez Colunga Lic. Elena Berenice Garza Hernández C.P. Aroldo Jiménez de la Cruz