GOBIERNO MUNICIPAL
PESQUERÍA, NUEVO LEÓN.

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES DE LA ADMINISTRACIÓN PÚBLICA MUNICIPAL DE PESQUERÍA, N.L. 2024-2027.

Presidencia Municipal
Morelos 100, Centro de Pesquería
Nuevo León, México. C.P. 66650
(825)-244-0780
www.pesqueria.gob.mx

INDICE

Contenido

Presidencia Municipal
Morelos 100, Centro de Pesquería
Nuevo León, México. C.P. 66650
(825)-244-0780
www.pesqueria.gob.mx

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 de los ciudadanos en posesión de la Administración Pública Municipal del Municipio de Pesquería, 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 Pesquería, a través de la Unidad de Transparencia, en conjunto con los encargados 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 realizó un sondeo a todo el personal que trata datos personales a través de los Enlaces de las Unidades Administrativas de la Administración Pública Municipal del Municipio de Pesquería, 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 contestado el sondeo, se analizó la información recabada, lo que permitió la creación de las medidas de seguridad. A partir de los inventarios iniciales de las bases de datos personales y diversas acciones, 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.

LINEAMIENTO DE PROTECCIÓN DE DATOS PERSONALES PARA LOS SUJETOS OBLIGADOS DEL ESTADO DE NUEVO LEÓN.

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 nuevas o faltantes.

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.

Articulo 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 e responsable.
- **Anonimización.-** Es el reducir al mínimo los riesgos de re identificación de los datos, manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personales, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización, no conlleva una distorsión de los datos reales.
- **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.
- **Bios.-** El Sistema Básico de Entrada/Salida o BIOS por sus siglas en inglés (Basic Input-Output System), es un software básico instalado en la placa base, que localiza y carga el sistema operativo en la memoria conocida como RAM por sus siglas en inglés (Random Access Memory), que es la que usa el procesador para recibir instrucciones y guardar resultados.
- **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 Pesquería.
- Encargado.- Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata catos 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 Pesquería, 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 Pesquería.
- Seguridad de la Información.- Preservación de la confidencialidad, integridad y disponibilidad de la información, asi 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 Pesquería), 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 16 del Reglamento de la Administración Pública Municipal de Pesquería, 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 Diz 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

I.- 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 Pesquería, 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 Interior de la Administración Pública Municipal del Municipio de Pesquería 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 asi 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, asi 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 Pesquería.

No.	DEPENDENCIA	INVENTARIO DE DATOS PERSONALES
1	Dirección de Educación y Cultura	Inventario Datos Personales Alumnos en Talleres.
2	DIF Municipal	Inventario Datos Personales Apoyo Alimentario.
3	DIF Municipal	Inventario Datos Personales Apoyo Alimentario 2-4 años.
4	Secretaría de Desarrollo Social y Humano	Inventario Datos Personales Apoyos.
5	Secretaría de Ayuntamiento	Inventario Datos Personales Cartas Varias.
6	Casa del Adulto Mayor	Inventario Datos Personales.
7	Dirección de Recursos Humanos	Inventario Datos Personales Empleados de Nomina.
8	Dirección de Regularización y Tenencia de la Tierra	Inventario Datos Personales Escrituración.

9	Dirección de Deportes	Inventario datos personales Inscripción de Equipos a Ligas Deportivas.
10	Secretaría de Servicios Primarios	Inventario Datos Personales Reporte.
11	Instituto Municipal de la Mujer	Inventario Datos Personales Reporte de Usuarias.
12	Dirección Juvenil	Inventario Datos Personales Servicio Social.
13	Servicio de Guardería Municipal	Inventario Datos Personales Servicio Guardería Municipal.
14	Dirección de Deportes	Inventario Datos Personales Servicio Gimnasio.
15	Dirección de Salud	Inventario Datos Personales Servicios.
16	SIPINNA	Inventario Datos Personales.
17	DIF Municipal	Inventario Datos Personales Unidad Básica de Rehabilitación.
18	Consejería Jurídica	Inventario Datos Personales Asesoría Jurídica Gratuita.
19	Instituto Municipal de la Mujer	Inventario-Datos-Personales Atención a la violencia Social Psicológica y Jurídico.
20	Secretaría de Desarrollo Social y Humano	Inventario Datos Personales Bolsa de trabajo y Brigadas de empleo.
21	CAIPA	Inventario Datos Personales.
22	Órgano interno de Control	Inventario Datos Personales Cedula Citatoria.
23	Secretaría de Seguridad Pública	Inventario Datos Personales Detenciones.
24	Unidad de Transparencia	Inventario Datos Personales Ejercicio Derechos ARCO.
25	Secretaria de Obras Públicas	Inventario Datos Personales Licencia de Construcción.
26	Secretaría de Seguridad Pública	Inventario Datos Personales Reclutamiento de Cadetes.
27	Secretaria de Desarrollo Urbano	Inventario Datos Personales Tramites Diversos Factibilidad de Uso de Suelo.
28	Secretaria de Desarrollo Urbano	Inventario Datos Personales Tramites Diversos Licencia de Uso de Edificación.

Liga electrónica donde se pueden consultar los inventarios de los datos personales cuyos tratamientos fueron descritos en las tablas previamente establecidas:

https://pesqueria.gob.mx/2021/05/13/realiza-una-solicitud-al-acceso-a-la-informacion-publica-o-derechos-arco/

II.- 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 Direcciones de cada dependencia y entidad de la Administración Pública Municipal, que participan en el tratamiento de los datos personales derivado de sus atribuciones.

La persona servidora pública involucrada en el tratamiento de datos personales deberá:

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 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 a los Lineamientos en materia de Protección de Datos Personales para los Sujetos Obligados del Municipio de Pesquería, en el tratamiento de datos personales.
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.

El servidor público responsable de cada proceso, o en su caso, el titular de la Unidad Administrativa responsable de cada tratamiento deberá:

1. Conocer y aplicar las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que poses los datos personales.
2. Conocer, aplicar y sujetarse al Aviso de Privacidad y a los Lineamientos en materia de Protección de Datos Personales para los Sujetos Obligados del Municipio de Pesquería, en el tratamiento de datos personales.

3. Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
4. Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.

5. Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.
6. Informar a la Di sobre los cambios que sufren sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, as medidas correctivas implementadas y las transferencias nuevas que realicen de los datos personales.
7. Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.
8. Informar a la DT, en caso de detectar alguna vulneración de datos personales.

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.
VIII. Son obligaciones del Comité de Transparencia en relación al tratamiento de datos personales, previstas en el artículo 38 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.

III.- ANALISIS DE RIESGOS

El análisis de riesgo tiene como objetivo alinear la protección de los datos personales que se traten en el Municipio de Pesquería, 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 Pesquería, 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 cario 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 Perdida 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 ➢ Identificaciones ➢ Documentos académicos ➢ Documentos patrimoniales ➢ Entre otros	**MEDIO**
Aspectos personales: ➢ Personas a grupos con los que se relaciona ➢ Temperamento ➢ Carácter ➢ Inteligencia ➢ 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**
Rendimiento laboral: ➢ Control de acceso al lugar de trabajo; ➢ Grabación de imágenes en zonas de acceso o en oficinas; ➢ Grabación de audio en zonas de acceso o en oficinas;	**MEDIO**

➢ 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.	
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 ➢ Historia clínica ➢ Informes de salud ➢ 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 menta ➢ 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 ➢ Facciones rostro ➢ Iris ➢ Venas de la palma de la mano ➢ Voz ➢ Oreja ➢ 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). ➢ Entre otros.	**MEDIO**
Datos de Identificación: ➢ Bajo ➢ Nombre ➢ Estado Civil ➢ Fecha de Nacimiento. ➢ Nacionalidad ➢ Lugar de nacimiento ➢ Domicilio ➢ Teléfono ➢ Correo electrónico ➢ Firma autógrafa ➢ Firma electrónica ➢ Edad ➢ imagen	**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 Pesquería, 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
Datos Migratorios	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 Pesquería 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 lodos 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 labora ➢ Monitorización por medio de imágenes en ámbito laboral	Medio	Información de lugar, tiempo y hora donde radican los servidores públicos, así como los cambios de tumos, modo y lugares de vigilancia.	+ 50,000	3

➢ 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 asi 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	Alto	Acceso no autorizado a la información relativa a la supervisión de actividades de las y los servidores públicos.	+ 50,000	3

➢ Análisis de transmisiones ➢ Análisis de Internet ➢ Control de tráfico rodado ➢ Entre otros que pudieran derivar.				
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 ➢ Derecho de petición	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 Pesquería.	+ 500,000	3

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 ➢ Derecho a la portabilidad	Alto	Privar de los derechos de los titulares en materia de protección de datos personales.	+ 500,000	3
Decidir sobre el acceso a un servicio de los que presta el Municipio de Pesquería.	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	
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	

DATOS PERSONALES				
Documentos Personales: ➢ Correos electrónicos ➢ Actas de Nacimiento ➢ Curp ➢ Identificaciones ➢ Documentos académicos ➢ Documentos patrimoniales 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 ➢ Temperamento ➢ Carácter ➢ Inteligencia ➢ 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,	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

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				
Rendimiento laboral: ➢ Control de acceso al lugar de trabaje ➢ Grabación de imágenes en zonas de acceso o en oficinas ➢ Grabación de audio en zonas de acceso o en oficinas. ➢ Monitorización de los equipos de los ➢ empleados ➢ 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, asi 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 (gastos en alimentación, Vivienda, educación, salud, impuestos,	Muy Alto	Puede ocasionar discriminación, o bien ser objetivos para fraudes o extorciones.	+ 5,000	5

pagos de créditos, tarjetas de crédito o gastos personales, etc; ➢ Nivel de deuda (Préstamos personales, hipotecas) ➢ Ingresos. Entre otros.				
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: ➢ Historia clínica ➢ Informes de salud	Alto	Pueden ser objeto de ataques a la privacidad personal, discriminación manipulación, o	+ 5,000	3

➢ Informes de baja laboral por motivos de salud para el servicio de Prevención de Riesgos Laborales ➢ Recetas medicas ➢ Datos relativos a salud física ➢ Datos relativos a salud mental ➢ Datos de la prestación de servicios de atención sanitaria ➢ Documentos relativos a procesos asistenciales del paciente (Incluida identificación de médicos y demás profesionales que han intervenido) en Cualquier Información que se Considere trascendental para el conocimiento veraz y actualizado de estado de salud del paciente. ➢ Datos Genéticos		Perjuicio moral.		
Datos biométricos: ➢ Huella dactilar ➢ Facciones rostro, Iris ➢ Venas de la palma de la mano ➢ Voz, Oreja, 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	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

➢ sexuales Entre otros.				
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 tráfico de 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). 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 ➢ Firma autógrafa ➢ Firma electrónica ➢ Edad imagen	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

IV. ANALISIS DE BRECHA

Para realizar el análisis de brecha, la Unidad de Transparencia dependiente de la Contraloría Municipal de Pesquería, elaboró y aplicó un sondeo con el objetivo de efectuar un auto

diagnostico 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 Pesquería se encuentra susceptible de enfrentar, se formula el presente análisis de brecha, utilizando como base el siguiente sondeo de Medidas de Seguridad:

MEDIDAS DE SEGURIDAD BASADAS EN LA CULTURA DEL PERSONAL:

¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?

[redacted]

¿Tienes mecanismos para eliminar de manera segura la información?

[redacted]

¿Has establecido y documentado los compromisos respecto a la protección de datos?

[redacted]

¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos Personales?

[redacted]

¿Realizas respaldos periódicos de los datos personales?

[redacted]

MEDIDAS DE SEGURIDAD EN EL ENTORNO DE TRABAJO FÍSICO:

¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?

[redacted]

¿Tienes medidas de seguridad para evitar el robo?

[redacted]

¿Cuidas los movimientos de información en entornos de trabajo físico?

[redacted]

MEDIDAS DE SEGURIDAD EN EL ENTORNO DE TRABAJO DIGITAL:

¿Realizas actualizaciones al equipo de cómputo?

[redacted]

¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?

[redacted]

¿Tienes medidas de seguridad para navegar en entornos digitales?

[redacted]

¿Cuidas el movimiento de información en entornos de trabajo digitales?

[redacted]

De igual manera, a fin de detectar las brechas de seguridad y determinar las medidas de seguridad que se implementan en el Municipio de Pesquería, se realizó y envió por parte de la DT, un sondeo a la Dirección de Soporte e Infraestructura de la Secretaria de Innovación y Gobierno Abierto del Municipio de Pesquería, quien es el área encargada de la seguridad informática, el cual se cita a continuación junto con las respuestas otorgadas por dicha Dirección:

¿Se tienen medidas de seguridad físicas, técnicas y administrativas para salvaguardar la información del servidor físico principal?

[redacted]

¿Se tiene un respaldo de toda la información en algún medio físico?

[redacted]

¿Se tiene Respaldo de toda la información en la nube?

[redacted]

RESPUESTA EN GENERAL FUE “SI”

¿Cuenta con medidas de contingencia ante ciberataques?

[redacted]

¿Revisa periódicamente el software instalado en los equipos de cómputo?

[redacted]

¿Revisa la configuración de la seguridad de todos las equipos de cómputo?

[redacted]

Señale que programas de seguridad informática se utilizan en el Municipio, describiendo los mismos, su configuración, sus actualizaciones contra virus y amenazas, y que protección tienen frente a ransomware.

[redacted]

En tal sentido, se tiene que el sistema de seguridad informática es acorde a las necesidades del Municipio de Pesquería, sin embargo, en cuanto a las actividades de las y las servidores públicos que dentro de sus funciones tratan datos personales, se detecta la necesidad de establecer un plan de trabajo a fin de solventar y mejorar la seguridad de la información personal que se encuentra en los sistemas de tratamiento del Municipio de Pesquería, motivo por el cual se plantea el siguiente:

V. PLAN DE TRABAJO.

La existencia del documento de seguridad, busca enmarcar los deberes de las Unidades Administrativas de las dependencias y entidades de la Administración Pública Municipal, para la máxima protección de datos personales. Debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan de trabajo es plasmar de manera enunciativa, más no limitativa, las actividades que las Unidades Administrativas de las dependencias y entidades de la Administración Pública Municipal, realizarán pera la aplicación del presente Documento de seguridad.
Lo anterior se realizará con base a las atribuciones establecidas en Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Nuevo León.

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

a) Se comunicará a los encargados, responsables y directores sobre la emisión del documento de seguridad y, se dará difusión en versión pública para el debido tratamiento de datos personales al interior de las Áreas del Municipio, de los Lineamientos en materia de Protección de Datos Personales para los Sujetos Obligados del Municipio de Pesquería.

b) Dar continuidad a los planes anuales de capacitación en materia de protección de datos personales dirigido a todas y todos los servidores públicos del Municipio de Pesquería, 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.

c) Enviar un comunicado electrónico al personal del Municipio de Pesquería en el cual se informará:

Los Lineamientos en materia de Protección de Datos Personales para los Sujetos Obligados del Municipio de Pesquería.

- Los conceptos básicos de la Protección de Datos Personales;
- Mejores prácticas para respaldar información; y
- Mantener actualizados los avisos de privacidad e inventario de datos personales.

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:

VI. MEDIDAS DE SEGURIDAD EN LA ADMINISTRACION PÚBLICA MUNICIPAL DE PESQUERÍA.

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 con protocolos de seguridad, que incluya, cuando menos, a designación de responsables por piso, procedimientos de control, señalizaciones y medidas

de protección física contra incendio, inundación, sismo, explosión y cualquier otra forma de desastre natural o humano.

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) Implementar programas de capacitación en materia de protección de datos personales al interior del Municipio.

MEDIDAS DE SEGURIDAD EN EL ENTORNO

Las Dependencias de la Administración Pública Municipal, deberán adoptar como mínimo las siguientes medidas de seguridad en el entorno, para evitar el acceso físico no autorizado a las instalaciones y a su información:

- ✓ Registrar a visitantes que accedan a instalaciones;
- ✓ Portar el gafete de visitante dentro de las instalaciones, por personas ajenas a la Administración Pública Municipal;
- ✓ Asegurar el retiro de pases de visita;
- ✓ Identificar a los servidores públicos adscritos al sujeto obligado, los cuales deberán portar la identificación deberá ser expedida y firmada por autoridad competente, e incluir cuando menos, nombre, cargo y número de empleado, fotografía, nombre de la Dependencia de su adscripción y unidad administrativa a la que pertenece, gafete de identificación dentro de las instalaciones.

MEDIDAS DE SEGURIDAD TÉCNICAS

Las medidas de seguridad técnicas consisten en mecanismos que se valen de la tecnología, aseguran el acceso a las bases de datos relacionados con el software y hardware, es decir protegen el entorno digital de los 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 que sea necesario al Área de informática de Municipio, para efectos del soporte informático requerido;
- Verificar que durante los mantenimientos y 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;
- Eliminar por completo del disco duro del equipo o cualquiera de sus dispositivos de almacenamiento, previamente a su devolución, tras la terminación del contrato respectivo, tratándose de arrendamiento o similar, o en caso de que sean dados de baja, toda la información que obre del sujeto obligado, particularmente, la que corresponde a datos personales, para que sólo quede bajo la custodia de las dependencias y entidades de la Administración Pública Municipal.
- 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 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.
- [redacted]
- [redacted]

MEDIDAS DE SEGURIDAD PARA PREVENIR ACCESOS NO AUTORIZADOS EN LAS INSTALACIONES.

Para prevenir el acceso no autorizado de las personas ajenas a las Unidades Administrativas de las Dependencias y Entidades de la Administración Pública Municipal, el personal que labora en oficialías de partes de cada dependencia deberá registrar a las personas y previa identificación, darle el acceso correspondiente con una tarjeta de visitante.

MEDIDAS DE SEGURIDAD EN CASO DE DESASTRES NATURALES.

Incendios y humos: Contar con detectores y sensores contra incendios, humos y gases, en las dependencias de la Administración Pública Municipal.

MEDIDAS DE SEGURIDAD CON RESPECTO A LA INFRAESTRUCTURA TECNOLÓGICA.

Con fundamento en el artículo 44 fracción VII y 51 del Reglamento de Gobierno del Municipio de Pesquería, Nuevo León, a través de la Coordinación de Sistemas es la unidad administrativa encargada de las medidas de seguridad con respecto a:

1) Amenazas externas en la red
2) Antivirus
3) Firewall
4) Instalación de software no autorizado
5) Servidores y sus copias de seguridad
6) Copias de seguridad o respaldos de la Información de los servidores

FORMAS DE SUPRESIÓN Y BORRADO SEGURO DE INFORMACIÓN, CUYO CONTENIDO SE ENCUENTRAN INMERSOS DATOS PERSONALES

Antes de establecer la modalidad de supresión y borrado seguro de la información, es indispensable precisar sobre su ciclo de vida, ya que es conforme a la baja documental que la Unidad Administrativa podrá realizar de acuerdo a las disposiciones que regulan la gestión documental al interior del Municipio.

Al tratarse de datos personales contenidos en archivos físicos y en sistemas electrónicos como en la nube, los riesgos que por la propia naturaleza tendría dicho sistema son: el uso indebido de la información, la falla en los equipos electrónicos o en los sistemas; por ello, el Municipio de Pesquería.

Cuenta con el apoyo de la Coordinación de Sistemas, quien es la encargada de ejecutar acciones para garantizar la Seguridad de la información.

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.

FISICAMENTE:

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.

LÓGICAMENTE:

Sobre-escritura.- esta consiste en sobre escribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información, nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

Anonimización.- Es el reducir al mínimo los riesgos de re identificación de los datos, manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personales, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización, no conlleva una distorsión de los datos reales.

VI. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Se podrán realizar verificaciones aleatorias en las Dependencias y Entidades de la Administración Pública, para conocer el grado de cumplimiento de las medidas de seguridad.

VII. EL PROGRAMA GENERAL DE CAPACITACIÓN

El programa de capacitaciones en materia de protección de datos personales se llevará a cabo de manera anual, cuyo objetivo primordial es el acercamiento del personal de la Administración Pública de Pesquería, a la materia de protección de datos personales, para tener una mayor comprensión de la responsabilidad que conlleva el trabajar con información personal de ciudadanos y trabajadores del Municipio, así como informar sobre las medidas de seguridad básicas que se deben de llevar a cabo para proteger la información que contiene datos personales.

VIII. ACTUALIZACIONES AL DOCUMENTO DE SEGURIDAD

El presente documento de seguridad se actualizará siguiendo las bases descritas en el artículo 42 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, cuando sucedan los siguientes acontecimientos.

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;

II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del Sistema de gestión,

III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y

IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Así lo acuerda, firma y Aprobado por el Comité de Transparencia de la Administración Pública del Municipio de Pesquería. Nuevo León, a los 29-veintinueve días del mes de enero de 2025-dos mil veinticinco.

COMITÉ DE TRANSPARENCIA
DEL MUNICIPIO DE PESQUERÍA, NUEVO LEÓN.

LIC. BALDOMERO JAVIER ELIZONDO SUAREZ
CONTRALOR MUNICIPAL Y PRESIDENTA
DEL COMITÉ DE TRANSPARENCIA

C. OSCAR GONZÁLEZ BONILLA
SECRETARIO DEL AYUNTAMIENTO Y
SECRETARIO DEL COMITÉ DE TRANSPARENCIA

C. MARÍA GRISELDA RODRÍGUEZ GARZA
SÍNDICO PRIMERO Y
VOCAL DEL COMITÉ DE TRANSPARENCIA