



Gobierno  
de  
—  
**Monterrey**

---

DOCUMENTO DE SEGURIDAD  
PARA LA PROTECCIÓN DE LOS  
DATOS PERSONALES DE LA  
ADMINISTRACIÓN PÚBLICA  
MUNICIPAL DE MONTERREY

---

2023



CONTENIDO

<b>INTRODUCCIÓN</b> .....	2
<b>MARCO NORMATIVO</b> .....	2
<b>GLOSARIO</b> .....	5
<b>I.- Inventarios de Datos Personales:</b> .....	8
<b>Catálogo de tratamiento de datos personales:</b> .....	10
<b>II.- Las Funciones y Obligaciones de las Personas que tratan Datos Personales:</b> .....	23
<b>III. ANÁLISIS DE RIESGOS:</b> .....	25
<b>IV. ANÁLISIS DE BRECHA:</b> .....	39
<b>V. PLAN DE TRABAJO:</b> .....	46
<b>VI. MEDIDAS DE SEGURIDAD EN LA ADMINISTRACIÓN PÚBLICA MUNICIPAL CENTRALIZADA Y LAS DEPENDENCIAS PARAMUNICIPALES DE MONTERREY.</b> .....	47
<b>Medidas de seguridad físicas y administrativas</b> .....	47
<b>Medidas de seguridad en el entorno</b> .....	48
<b>Medidas de seguridad técnicas</b> .....	48
<b>Medidas de seguridad para prevenir accesos no autorizados en las instalaciones</b> .....	49
<b>Medidas de seguridad en caso de desastres naturales:</b> .....	49
<b>Medidas de seguridad con respecto a la infraestructura tecnológica:</b> .....	49
<b>Formas de supresión y borrado seguro de información, cuyo contenido se encuentran inmersos datos personales</b> .....	50
<b>VII. EL PROGRAMA GENERAL DE CAPACITACIÓN</b> .....	50
<b>VIII. ACTUALIZACIONES AL DOCUMENTO DE SEGURIDAD</b> .....	51





## 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 Monterrey, Centralizada y Paramunicipal, como sujetos obligados, teniendo como base dicha normatividad, y en 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.

El precitado numeral señala que el documento de seguridad deberá contener por lo menos el inventario de datos personales; las funciones y obligaciones de las personas que traten datos personales; el análisis de riesgos; 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 Monterrey, a través de la Dirección 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 cuestionario a todo el personal que trata datos personales a través de los Titulares de las Unidades Administrativas de la Administración Pública Municipal del Municipio de Monterrey y sus Paramunicipales, 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 cuestionario, 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.

## 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.

### **Lineamientos 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 111, 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 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 del análisis de brecha, el responsable deberá considerar lo siguiente:

- I. Las medidas de seguridad existentes y efectivas;
- II. Las medidas de seguridad faltantes; y
- III. La existencia de nuevas medidas de seguridad que pudieran 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 aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- VI. El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- VII. Los incidentes y vulneraciones de seguridad ocurridas.



**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.

- **Anonimización:** Es el reducir al mínimo los riesgos de reidentificación 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.
- **DT:** Dirección de Transparencia de la Contraloría Municipal de Monterrey.
- **Encargado:** Persona física o jurídica, pública o privada, ajena 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 Monterrey, 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 Monterrey.
- **Sistema de Resolución de Nombres (DNS):** Es un protocolo transversal en los servicios de internet, las consideraciones en la privacidad deben tenerse en cuenta por un gran número de implicaciones desde los desarrolladores de software, administradores de red, los propios prestadores de servicio DNS y, proveedores de acceso a internet.
- **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 Monterrey o dependencia Paramunicipal), 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 Monterrey, Nuevo León, o a las Entidades de la Administración Pública Paramunicipal; 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.

#### 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 Monterrey y sus Paramunicipales, 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 Monterrey y la normativa que rige a sus Paramunicipales, 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 I, 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, género, 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, título, cédula profesional, certificados y reconocimientos.
- **Datos patrimoniales y/o financieros:** bienes muebles, bienes inmuebles, ingresos, egresos 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, diagnóstico, 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 Centralizada y Paramunicipal.
- Personas externas que prestan algún servicio para las Direcciones de cada dependencia y entidad de la Administración Pública Municipal Centralizada y Paramunicipal.
- Personas externas que participan en actividades que llevan a cabo las direcciones de la Administración Pública Municipal del Municipio de Monterrey y las dependencias Paramunicipales (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 Centralizada del Municipio de Monterrey.

Contraloría Municipal	CÁMARAS DE CIRCUITO CERRADO DE VIGILANCIA, PALACIO MUNICIPAL DE MONTERREY
Contraloría Municipal	CAPACITACIÓN PRESENCIAL
Contraloría Municipal	CAPACITACIÓN VIRTUAL IMPARTIDA POR EL INAI
Contraloría Municipal	COMISIÓN DE HONOR Y JUSTICIA DEL MUNICIPIO DE MONTERREY
Contraloría Municipal	CONSEJO CIUDADANO PARA EL GOBIERNO ABIERTO, LA TRANSPARENCIA Y RENDICIÓN DE CUENTAS
Contraloría Municipal	DENUNCIAS CONTRA SERVIDORES PÚBLICOS DEL MUNICIPIO DE MONTERREY
Contraloría Municipal	IMPLEMENTACIÓN DEL SISTEMA DE CONTROL INTERNO INSTITUCIONAL EN EL MUNICIPIO DE MONTERREY
Contraloría Municipal	RECEPCIÓN Y ATENCIÓN DE DUDAS Y QUEJAS DE LOS TITULARES SOBRE EL TRATAMIENTO DE SUS DATOS PERSONALES
Contraloría Municipal	REGISTRO DE DENUNCIAS CONTRA SERVIDORES PÚBLICOS EN LÍNEA
Contraloría Municipal	SOLICITUDES DE ACCESO A LA INFORMACIÓN PRESENTADA MEDIANTE MODALIDAD DIVERSA A LA PLATAFORMA NACIONAL DE TRANSPARENCIA -PNT
Contraloría Municipal	SOLICITUDES DE EJERCICIO DE DERECHOS ARCO – ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN
Contraloría Municipal	SUBSTANCIACIÓN Y RESOLUCIÓN DE PROCEDIMIENTOS DE RESPONSABILIDAD ADMINISTRATIVA
Contraloría Municipal	REGISTRO DE VISITANTES A LA CONTRALORÍA MUNICIPAL
Secretaría de Desarrollo Económico	PROGRAMA DE EMPLEO TEMPORAL
Secretaría de Desarrollo Económico	REGISTRO AL PROGRAMA DE DESARROLLO DE PROVEEDORES LOCALES.
Secretaría de Desarrollo Económico	REGISTRO CENTRO EMPRENDEMOS MONTERREY
Secretaría de Desarrollo Económico	REGISTRO DE INSCRIPCIÓN A LA FERIA AHORA EMPRENDEMOS JUNTAS Y JUNTOS.
Secretaría de Desarrollo Económico	REGISTRO DE INSCRIPCIÓN A PROGRAMA DE MICROCRÉDITOS EMPRENDE AHORA MONTERREY
Secretaría de Desarrollo Económico	REGISTRO DE INSCRIPCIÓN A PROGRAMA DE PROYECTOS PRODUCTIVOS AHORA EMPRENDEMOS JUNTOS



## Documento de Seguridad para la Protección de los Datos Personales

Secretaría de Desarrollo Económico	REGISTRO DE INSCRIPCIÓN A PROGRAMAS DE CAPACITACIÓN DE LA SECRETARÍA DE DESARROLLO ECONÓMICO DE MONTERREY.
Secretaría de Desarrollo Económico	AGENDA DISFRUTA MONTERREY
Secretaría de Desarrollo Humano e Igualdad Sustantiva	21, 10, 5 Y 1K FUNDACIÓN MONTERREY
Secretaría de Desarrollo Humano e Igualdad Sustantiva	AHORA BAILEMOS
Secretaría de Desarrollo Humano e Igualdad Sustantiva	ATENCIÓN A LAS VIVIENDAS
Secretaría de Desarrollo Humano e Igualdad Sustantiva	BECAS
Secretaría de Desarrollo Humano e Igualdad Sustantiva	CARRERAS INFANTILES
Secretaría de Desarrollo Humano e Igualdad Sustantiva	DÍA DE LA MAESTRA Y EL MAESTRO
Secretaría de Desarrollo Humano e Igualdad Sustantiva	DIAGNÓSTICO DE MEDICIÓN MULTIDIMENSIONAL DE POBREZA
Secretaría de Desarrollo Humano e Igualdad Sustantiva	DILIGENCIAS DE JURISDICCIÓN VOLUNTARIA
Secretaría de Desarrollo Humano e Igualdad Sustantiva	ENCUESTA PARA TRABAJADORES EN LA RECOLECCIÓN ALTERNA
Secretaría de Desarrollo Humano e Igualdad Sustantiva	ENTREGA DE ÚTILES ESCOLARES
Secretaría de Desarrollo Humano e Igualdad Sustantiva	ESPACIO CERO CINCO
Secretaría de Desarrollo Humano e Igualdad Sustantiva	FORO DE VINCULACIÓN PARA LA INCLUSIÓN DE PERSONAS CON DISCAPACIDAD





Secretaría de Desarrollo Humano e Igualdad Sustantiva	JUICIO DE TRANSMISIÓN HEREDITARIA
Secretaría de Desarrollo Humano e Igualdad Sustantiva	JUICIO SUCESORIO DE INTESTADO ESPECIAL
Secretaría de Desarrollo Humano e Igualdad Sustantiva	JUNTAS Y JUNTOS POR TU ESCUELA
Secretaría de Desarrollo Humano e Igualdad Sustantiva	MODELO DE ATENCIÓN INTEGRAL
Secretaría de Desarrollo Humano e Igualdad Sustantiva	MUSEO METROPOLITANO
Secretaría de Desarrollo Humano e Igualdad Sustantiva	PREMIO AL DEPORTE 2021
Secretaría de Desarrollo Humano e Igualdad Sustantiva	PROMOCIÓN E IMPULSO AL DEPORTE Y LA CREACIÓN
Secretaría de Desarrollo Humano e Igualdad Sustantiva	PROMOCIÓN E IMPULSO AL DESARROLLO CULTURAL
Secretaría de Desarrollo Humano e Igualdad Sustantiva	RECTIFICACIÓN DE ACTAS
Secretaría de Desarrollo Humano e Igualdad Sustantiva	REGISTRO DE PERSONAS BENEFICIARIAS DEL PROGRAMA CONTIGO MONTERREY
Secretaría de Desarrollo Humano e Igualdad Sustantiva	ROSA DE LOS VIENTOS
Secretaría de Desarrollo Humano e Igualdad Sustantiva	TESTAMENTO
Secretaría de Desarrollo Humano e Igualdad Sustantiva	VIERNES GAMER
Secretaría de Desarrollo Humano e Igualdad Sustantiva	ADOPCIONES DE ANIMALES DE COMPAÑÍA



## Documento de Seguridad para la Protección de los Datos Personales

Secretaría de Desarrollo Humano e Igualdad Sustantiva	REUNIONES SOBRE BIENESTAR ANIMAL
Secretaría de Desarrollo Humano e Igualdad Sustantiva	ALBERGUE PARA PERSONAS MIGRANTES INTERNACIONALES
Secretaría de Desarrollo Humano e Igualdad Sustantiva	ATENCIÓN INTEGRAL CONTRA LA POBREZA
Secretaría de Desarrollo Humano e Igualdad Sustantiva	GANADORES DE REGALOS POR EL FESTEJO "EL PAPÁ+PADRE"
Secretaría de Desarrollo Humano e Igualdad Sustantiva	DIRECCIÓN DE ENLACE "SOLICITUDES Y PETICIONES"
Secretaría de Desarrollo Humano e Igualdad Sustantiva	EVENTOS DE SENSIBILIZACIÓN SOBRE DERECHOS HUMANOS, PERSPECTIVA DE GÉNERO E IGUALDAD SUSTANTIVA
Secretaría de Desarrollo Humano e Igualdad Sustantiva	EVENTOS DE ATENCIÓN INTEGRAL DIRIGIDAS A POBLACIÓN EN CONTEXTO DE MOVILIDAD
Secretaría de Desarrollo Humano e Igualdad Sustantiva	CAPACITACIÓN Y TALLERES DE SENSIBILIZACIÓN SOBRE DERECHOS HUMANOS, PERSPECTIVA DE GÉNERO E IGUALDAD SUSTANTIVA DIRIGIDO A PERSONAS SERVIDORAS PÚBLICAS DE LA ADMINISTRACIÓN PÚBLICA DE MONTERREY
Secretaría de Desarrollo Humano e Igualdad Sustantiva	COMUNIDADES SALUDABLES
Secretaría de Desarrollo Humano e Igualdad Sustantiva	CONSEJO DE LA NIÑEZ
Secretaría de Desarrollo Humano e Igualdad Sustantiva	PROMOCIÓN DE LA SALUD
Secretaría de Desarrollo Humano e Igualdad Sustantiva	PROMOVIENDO UN AMBIENTE LABORAL IGUALITARIO PARA PERSONAL DEL AYUNTAMIENTO
Secretaría de Desarrollo Humano e Igualdad Sustantiva	USO DE LICENCIAS CON Y SIN GOCE DE SUELDO EN LA ADMINISTRACIÓN PÚBLICA MUNICIPAL DE MONTERREY
Secretaría de Desarrollo Humano e Igualdad Sustantiva	USO DE LICENCIA CON GOCE POR PATERNIDAD





Secretaría de Desarrollo Urbano Sostenible	ALINEAMIENTO VIAL
Secretaría de Desarrollo Urbano Sostenible	ANUNCIOS PUBLICITARIOS
Secretaría de Desarrollo Urbano Sostenible	AUTORIZACIÓN DEL PROYECTO DE VENTAS
Secretaría de Desarrollo Urbano Sostenible	CONSTANCIA DE TERMINACION DE OBRAS
Secretaría de Desarrollo Urbano Sostenible	CONSTANCIA DE TERMINACION DE OBRAS EN CONDOMINIO Y LIBERACIÓN DE GARANTIAS
Secretaría de Desarrollo Urbano Sostenible	CONSTANCIA DE TERMINACIÓN DE OBRAS Y LIBERACION DE GARANTIAS
Secretaría de Desarrollo Urbano Sostenible	DEMOLICIÓN PARCIAL (HASTA 200 M2 DE CONSTRUCCIÓN)
Secretaría de Desarrollo Urbano Sostenible	DEMOLICIÓN PARCIAL (MAYOR DE 200 M2 DE CONSTRUCCIÓN)
Secretaría de Desarrollo Urbano Sostenible	DEMOLICIÓN TOTAL (HASTA 200 M2 DE CONSTRUCCIÓN)
Secretaría de Desarrollo Urbano Sostenible	DEMOLICIÓN TOTAL (MAYOR DE 200 M2 DE CONSTRUCCIÓN)
Secretaría de Desarrollo Urbano Sostenible	DERRIBO, PODA, DESYERBE, TRASPLANTE
Secretaría de Desarrollo Urbano Sostenible	ENLACE Y ATENCIÓN INSTITUCIONAL DE LA SECRETARÍA, CON LA EJECUTIVA, CON LA SECRETARÍA DE FINANZAS Y ADMINISTRACIÓN, CON CONTRALORIA MUNICIPAL Y CON LA DIRECCIÓN DE AUSTOS JURIDICOS DEL AYUNTAMIENTO.
Secretaría de Desarrollo Urbano Sostenible	ESTACIONAMIENTOS EXCLUSIVOS, NOMECLATURAS, ANUENCIA PARA CNSTRUCCION DE PUENTES PEATONALES
Secretaría de Desarrollo Urbano Sostenible	ESTRATEGIAS, PROGRAMAS Y PROYECTOS PARA LA MOVIIDAD EFICIENTE, INTEGRADA, ACCESIBLE, SEGURA Y SOSTENIBLE; FOMENTANDO Y PRIORIZANDO EL USO DEL TRANSPORTE PUBLICO Y LOS MODOS NO MOTORIZADOS.
Secretaría de Desarrollo Urbano Sostenible	FACTIBILIDAD DE FRACCIONAR Y URBANIZAR EL SUELO
Secretaría de Desarrollo Urbano Sostenible	FACTIBILIDAD DE USO DE SUELO
Secretaría de Desarrollo Urbano Sostenible	FACTIBILIDAD DE USO DE SUELO, FIJACIÓN DE LINEAMIENTOS GENERALES DEL DISEÑO ARQUITECTÓNICO Y LICENCIA DE USO DE SUELO
Secretaría de Desarrollo Urbano Sostenible	FIJACIÓN DE LINEAMIENTOS GENERALES DEL DISEÑO ARQUITECTÓNICO
Secretaría de Desarrollo Urbano Sostenible	FRACCIONAMIENTOS, FUSIONES, PARCELACIONES, RELOTIFICACIONES, SUBDIVISIONES, CONJUNTOS URBANOS



## Documento de Seguridad para la Protección de los Datos Personales

Secretaría de Desarrollo Urbano Sostenible	LICENCIA DE CONSTRUCCIÓN OBRA NUEVA
Secretaría de Desarrollo Urbano Sostenible	LICENCIA DE CONSTRUCCIÓN PARA BARDA MAYOR A 3 MTS DE ALTURA
Secretaría de Desarrollo Urbano Sostenible	LICENCIA DE CONSTRUCCIÓN PARA BARDA MENOR A 3 MTS DE ALTURA
Secretaría de Desarrollo Urbano Sostenible	LICENCIA DE CONSTRUCCIÓN PARA OBRA NUEVA, AMPIACIÓN REGULARIZACIÓN DE CASA HABITACION UNIFAMILIAR CON PENDIENTE DE CONTENCIÓN HASTA 3.5MTS DE ALTURA
Secretaría de Desarrollo Urbano Sostenible	LICENCIA DE USO COMPLEMENTARIO A LA VIVIENDA
Secretaría de Desarrollo Urbano Sostenible	LICENCIA DE USO DE EDIFICACIÓN
Secretaría de Desarrollo Urbano Sostenible	LICENCIA DE USO DE EDIFICACIÓN(SARE)
Secretaría de Desarrollo Urbano Sostenible	LICENCIA DE USO DE SUELO
Secretaría de Desarrollo Urbano Sostenible	LINEAMIENTOS GENERALES DEL DISEÑO URBANO
Secretaría de Desarrollo Urbano Sostenible	MUNICIPALIZACIÓN
Secretaría de Desarrollo Urbano Sostenible	PLANO DE RASANTES
Secretaría de Desarrollo Urbano Sostenible	PRORROGA PARA LA TERMINACIÓN DE OBRAS
Secretaría de Desarrollo Urbano Sostenible	PROYECTO DE VENTAS EN CONDOMINIO (REGIMEN EN CONDOMINIOS MIXTOS) Y CONSTANCIA DE TERMINACIÓN DE OBRAS.
Secretaría de Desarrollo Urbano Sostenible	PROYECTO DE VENTAS EN CONDOMINIO Y GARANTIA SUFICIENTE
Secretaría de Desarrollo Urbano Sostenible	PROYECTO EJECUTIVO ARQUITECTÓNICO O LICENCIA DE CONSTRUCCIÓN
Secretaría de Desarrollo Urbano Sostenible	PROYECTO EJECUTIVO ARQUITECTÓNICO O LICENCIA DE CONSTRUCCIÓN, PROYECTO DE VENTAS EN CONDOMINIO(RÉGIMEN EN CONDOMINIOS MIXTOS)
Secretaría de Desarrollo Urbano Sostenible	PROYECTO EJECUTIVO URBANISTICO Y/O SU MODIFICACIÓN
Secretaría de Desarrollo Urbano Sostenible	REGULARIZACIÓN DE LA TENENCIA DE LA TIERRA DE UN ASENTAMIENTO IRREGULAR
Secretaría de Desarrollo Urbano Sostenible	REMODELACIÓN DE FACHADA
Secretaría de Desarrollo Urbano Sostenible	SUBDIVISIONES, FUSIONES, PARECLACIONES Y RELOTIFICACIONES





**Documento de Seguridad para la Protección de los Datos Personales**

Secretaría de Desarrollo Urbano Sostenible	USO DE SUELO, USO DE EDIFICACION, CONSTRUCCION , REGIMEN DE COMDOMINIO, NUMERO OFICIAL.
Secretaría de Desarrollo Urbano Sostenible	TRAMITES ADMINISTRATIVOS
Secretaría de Desarrollo Urbano Sostenible	ACUERDO VERDE
Secretaría de Desarrollo Urbano Sostenible	CONVOCATORIA PARA INTEHRACIÓN DEL CONSEJO CONSULTORIO DE MOVILIDAD
Secretaría de Desarrollo Urbano Sostenible	DESARROLLO URBANO Y ECOLOGIA
Secretaría de Desarrollo Urbano Sostenible	CONTROL URBANO
Secretaría de Desarrollo Urbano Sostenible	PROYECTOS TECNICOS
Secretaría de Desarrollo Urbano Sostenible	DIRECCIÓN PARA UN DESARROLLO COMPACTO
Secretaría de Desarrollo Urbano Sostenible	CAMARAS DE CIRCUITO CERRADO SEDUSO
Secretaría de Finanzas y Administración	CONSTANCIAS DE NO AFECTACIÓN A BIENES DE DOMINIO PÚBLICO MUNICIPAL Y CONSTANCIA DE IDENTIFICACIÓN DE ÁREAS MUNICIPALES
Secretaría de Finanzas y Administración	FORMATO IMPRESO DE CARTA PODER
Secretaría de Finanzas y Administración	INTEGRACIÓN DE EXPEDIENTES LABORALES
Secretaría de Finanzas y Administración	INTEGRACIÓN Y ACTUALIZACIÓN DEL PADRÓN MUNICIPAL DE CONTRIBUYENTES. PAGO DE IMPUESTO PREDIAL, PAGO DEL IMPUESTO SOBRE LA ADQUISICIÓN DE INMUEBLES, TRAMITE DE TARIFA ÚNICA ESPECIAL, INSPECCIÓN DE LOTES BALDÍOS
Secretaría de Finanzas y Administración	PROCEDIMIENTO
Secretaría de Finanzas y Administración	PROVEEDORES
Secretaría de Finanzas y Administración	SERVICIOS MÉDICOS
Secretaría de Finanzas y Administración	PAGO DE IMPUESTOS, APROVECHAMIENTOS, DERECHOS Y MULTAS POR PARTE DE PERSONAS FÍSICAS Y MORALES
Secretaría de Finanzas y Administración	PAGO DE CHEQUES Y RESGUARDO DE RECIBOS DE NÓMINA
Secretaría de Finanzas y Administración	PROREGIO EMPRESARIAL
Secretaría de Finanzas y Administración	CERTIFICADO DE NO ADEUDO DE IMPUESTO PREDIAL



## Documento de Seguridad para la Protección de los Datos Personales

Secretaría de Finanzas y Administración	PRÓRROGA EN EL CÁLCULO DEL IMPUESTO PREDIAL SOBRE LA CONSTRUCCIÓN NO TERMINADA
Secretaría de Finanzas y Administración	APOYOS CONFORME A LAS BASES GENERALES PARA EL OTORGAMIENTO DE SUBSIDIOS CON CARGO AL ERARIO MUNICIPAL
Secretaría de Finanzas y Administración	REFRENDO EN EL CATÁLOGO DE PROVEEDORES Y PRESTADORES DE SERVICIO DEL MUNICIPIO DE MONTERREY
Secretaría de Infraestructura Sostenible	LIBRO DE VISITAS
Secretaría de Infraestructura Sostenible	PARTICIPACION SOCIAL
Secretaría de Innovación y Gobierno Abierto	MONTERREY CIUDAD DIGITAL
Secretaría de Innovación y Gobierno Abierto	ASAMBLEAS CIUDADANAS
Secretaría de Innovación y Gobierno Abierto	BUZÓN DE SUGERENCIA Y ASESORÍA DE TRÁMITES Y SERVICIOS
Secretaría de Innovación y Gobierno Abierto	ENTRADAS Y SALIDAS A LAS INSTALACIONES DE LA SECRETARÍA DE INNOVACIÓN Y GOBIERNO ABIERTO
Secretaría de Innovación y Gobierno Abierto	HERRAMIENTA DE ENCUESTA CIUDADANA
Secretaría de Innovación y Gobierno Abierto	PREMIO SIGA
Secretaría de Innovación y Gobierno Abierto	PROTESTA CIUDADANA
Secretaría de Innovación y Gobierno Abierto	RESTRICCIÓN TEMPORAL DE ACCESO A UNA VÍA PÚBLICA
Secretaría de Innovación y Gobierno Abierto	SERVICIO DE JUNTAS VECINALES
Secretaría de Innovación y Gobierno Abierto	VALIDACIÓN EN LA PLATAFORMA DE INTERNET DEL PRESUPUESTO PARTICIPATIVO
Secretaría de Innovación y Gobierno Abierto	CAPACITACIÓN PRESENCIAL Y MODALIDAD EN LÍNEA
Secretaría de Seguridad Ciudadana	ATENCIÓN A VÍCTIMAS DE VIOLENCIA FAMILIAR Y DE GÉNERO
Secretaría de Seguridad Ciudadana	DETENIDOS
Secretaría de Seguridad Ciudadana	EXPEDICIÓN DE PERMISOS DE CARGA Y DESCARGA, EXCESO DE DIMENSIONES, VÍAS LIMITADAS
Secretaría de Seguridad Ciudadana	MULTAS DE TRÁNSITO
Secretaría de Seguridad Ciudadana	PREVENCIÓN DE LA VIOLENCIA Y DELINCUENCIA JUVENIL





## Documento de Seguridad para la Protección de los Datos Personales

Secretaría de Seguridad Ciudadana	RESPIRA MONTERREY
Secretaría de Servicios Públicos	PERMISO PARA LA CONSTRUCCIÓN DE CERCOS O GAVETAS
Secretaría de Servicios Públicos	AHORA NOS DIVERTIMOS JUNTOS
Secretaría de Servicios Públicos	AUTORIZACIÓN PARA PERSONAS FÍSICAS O MORALES CON VEHÍCULOS DESTINADOS AL SERVICIO PRIVADO DE RECOLECCIÓN Y TRASLADO DE RESIDUOS NO PELIGROSOS EN EL TERRITORIO MUNICIPAL DE MONTERREY.
Secretaría de Servicios Públicos	CAMPAMENTOS DE VERANO
Secretaría de Servicios Públicos	CREMACIÓN
Secretaría de Servicios Públicos	ENTREGA DE PREMIOS
Secretaría de Servicios Públicos	EXHUMACIÓN
Secretaría de Servicios Públicos	INHUMACIÓN
Secretaría de Servicios Públicos	ORDEN PARA EXPLOTACIÓN DE BIENES MUNICIPALES
Secretaría de Servicios Públicos	PERMISO DE CONSTRUCCIÓN EN VÍA PÚBLICA
Secretaría de Servicios Públicos	RE-INHUMACIÓN
Secretaría de Servicios Públicos	RENTA DE LOTES DE PANTEONES MUNICIPALES
Secretaría de Servicios Públicos	RENTA DE MEDIDORES COLECTIVOS
Secretaría de Servicios Públicos	REPORTES PRESENTADOS ANTE LA SECRETARÍA DE SERVICIOS PÚBLICOS
Secretaría de Servicios Públicos	SOLICITUD DE SERVICIO DE RECOLECCIÓN DE RESIDUOS SÓLIDOS NO PELIGROSOS A ESTABLECIMIENTOS TIPO A (ESTABLECIMIENTOS INDUSTRIALES, COMERCIALES Y DE SERVICIOS QUE GENEREN HASTA DE 0 A 5 KG DE RESIDUOS SÓLIDOS NO PELIGROSOS DIARIOS EN PROMEDIO.)
Secretaría de Servicios Públicos	SOLICITUD DE SERVICIO DE RECOLECCIÓN DE RESIDUOS SÓLIDOS NO PELIGROSOS A ESTABLECIMIENTOS TIPO C (ESTABLECIMIENTOS EN CASA HABITACIÓN)
Secretaría de Servicios Públicos	SOLICITUD DE SERVICIO DE RECOLECCIÓN DE RESIDUOS SÓLIDOS NO PELIGROSOS TIPO B (ESTABLECIMIENTOS INDUSTRIALES, COMERCIALES Y DE SERVICIOS QUE GENEREN MÁS DE 5 KG. Y HASTA 10 KG DE RESIDUOS SÓLIDOS NO PELIGROSOS DIARIOS EN PROMEDIO.)





Secretaría del Ayuntamiento	"SEBRADORES DE PAZ"
Secretaría del Ayuntamiento	BASE DE DATOS ANUENCIA MUNICIPAL
Secretaría del Ayuntamiento	BASE DE DATOS ASESORIA JURÍDICA
Secretaría del Ayuntamiento	BASE DE DATOS AUDIENCIAS CON EL ALCALDE
Secretaría del Ayuntamiento	BASE DE DATOS CONSEJOS CONSULTIVOS CIUDADANOS
Secretaría del Ayuntamiento	BASE DE DATOS CONSULTAS PÚBLICAS REGLAMENTOS
Secretaría del Ayuntamiento	BASE DE DATOS DE CARTILLA DE IDENTIDAD MILITAR
Secretaría del Ayuntamiento	BASE DE DATOS DE EXPEDICIÓN Y/O RENOVACIÓN DEL PASAPORTE MEXICANO
Secretaría del Ayuntamiento	BASE DE DATOS DEL DIAGNOSTICO TENDIENTE A LA REGULARIZACIÓN Y REUBICACIÓN DEL EJERCICIO DE LA ACTIVIDAD COMERCIAL
Secretaría del Ayuntamiento	BASE DE DATOS DERECHO DE PETICIÓN
Secretaría del Ayuntamiento	BASE DE DATOS EMISIÓN DE CONSULTA Y BÚSQUEDA DE DOCUMENTOS QUE OBRAN EN EL ARCHIVO HISTORICO
Secretaría del Ayuntamiento	BASE DE DATOS EMISIÓN DE CONSULTA, BÚSQUEDA Y REPRODUCCIÓN DE DOCUMENTOS
Secretaría del Ayuntamiento	BASE DE DATOS EMISIÓN DE COPIAS CERTIFICADAS
Secretaría del Ayuntamiento	BASE DE DATOS EMISIÓN DE COPIAS SIMPLES
Secretaría del Ayuntamiento	BASE DE DATOS ENTREGA DE MEDALLAS Y RECONOCIMIENTOS
Secretaría del Ayuntamiento	BASE DE DATOS EXPEDICIÓN DE CARTA CERTIFICADA SUSCRITA POR JUEZ AUXILIAR
Secretaría del Ayuntamiento	BASE DE DATOS EXPEDICIÓN DE CARTA SIMPLE SUSCRITA POR JUEZ AUXILIAR
Secretaría del Ayuntamiento	BASE DE DATOS GESTIÓN SOCIAL Y RESOLUCIÓN DE PROBLEMATICAS SOCIALES.
Secretaría del Ayuntamiento	BASE DE DATOS INVASIÓN DE TERRENOS MUNICIPALES
Secretaría del Ayuntamiento	BASE DE DATOS ORIENTACIÓN A GRUPOS RELIGIOSOS
Secretaría del Ayuntamiento	BASE DE DATOS PERMISO DE ESPECTACULOS
Secretaría del Ayuntamiento	BASE DE DATOS PERMISO PARA EL USO DE LA VÍA PÚBLICA EN EL EJERCICIO DE LA ACTIVIDAD COMERCIAL
Secretaría del Ayuntamiento	BASE DE DATOS PERMISO PARA PERMISO DE USO TEMPORAL DE ESPACIOS PÚBLICOS MUNICIPALES
Secretaría del Ayuntamiento	BASE DE DATOS RECURSO DE INCONFORMIDAD E INDEMNIZACIÓN
Secretaría del Ayuntamiento	BASE DE DATOS RECURSO DE REVISIÓN EN MATERIA DE DESARROLLO URBANO
Secretaría del Ayuntamiento	BÚSQUEDA DE INFORMACIÓN Y LOCALIZACIÓN EN ACTAS DE CABILDO, GACETA MUNICIPAL Y REGLAMENTOS MUNICIPALES
Secretaría del Ayuntamiento	LIBRO DE REGISTRO DE VISITAS DE LAS OFICINAS DE LA SECRETARÍA DEL AYUNTAMIENTO
Secretaría del Ayuntamiento	LIBRO DE REGISTRO DE VISITAS DE LAS OFICINAS DE LA DIRECCIÓN GENERAL DE CONTROL REGULATORIO Y VIGILANCIA DE LA SECRETARÍA DEL AYUNTAMIENTO
Secretaría del Ayuntamiento	SERVICIO DE MEDIACIÓN
Secretaría del Ayuntamiento	DIFUSIÓN DE DATOS DE CONTACTO DE LAS JUEZAS Y JUECES AUXILIARES SELECCIONADOS A TRAVÉS DEL PROGRAMA DENOMINADO "SEBRADORES DE PAZ"





## Documento de Seguridad para la Protección de los Datos Personales

Secretaría del Ayuntamiento	CONSULTA CIUDADANA DE JUEZAS Y JUECES AUXILIARES SELECCIONADOS A TRAVÉS DEL PROGRAMA DENOMINADO "SEMBRADORES DE PAZ"
Secretaría del Ayuntamiento	CONVOCATORIA PÚBLICA PARA CONFORMAR EL SEGUNDO PARLAMENTO JUVENIL DEL MUNICIPIO DE MONTERREY
Secretaría Ejecutiva	AHORA RESOLVEMOS JUNTOS
Secretaría Ejecutiva	RECEPCIÓN EJECUTIVA
Secretaría Ejecutiva	GESTIÓN DE AGENDA
Síndicos y Regidores	ATENCIÓN Y ORIENTACIÓN CIUDADANA
Síndicos y Regidores	SUBSIDIOS DE IMPUESTOS Y MULTAS
Sistema para el Desarrollo Integral de la Familia	TALLER PRODUCTIVO
Sistema para el Desarrollo Integral de la Familia	ACTIVIDADES DE LOS CEDIF.
Sistema para el Desarrollo Integral de la Familia	ASESORÍA JURÍDICA ESPECIALIZADA
Sistema para el Desarrollo Integral de la Familia	ATENCIÓN A CASOS ASISTENCIALES
Sistema para el Desarrollo Integral de la Familia	ATENCIÓN A REPORTES DE PERSONAS ADULTAS MAYORES EN RIESGO
Sistema para el Desarrollo Integral de la Familia	CLÍNICA DE ATENCIÓN INTEGRAL AL AUTISMO
Sistema para el Desarrollo Integral de la Familia	CONSTANCIA DE ACTIVIDADES ASISTENCIALES
Sistema para el Desarrollo Integral de la Familia	DEFENSORÍA MUNICIPAL PARA LA PROTECCIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES
Sistema para el Desarrollo Integral de la Familia	ESPACIOS INFANCIA-ADOLESCENCIA
Sistema para el Desarrollo Integral de la Familia	ESTANCIA INFANTIL
Sistema para el Desarrollo Integral de la Familia	GUARDERÍA ESPECIAL
Sistema para el Desarrollo Integral de la Familia	LUDOTECA INFANTIL
Sistema para el Desarrollo Integral de la Familia	PROGRAMA DE ATENCIÓN A LA POBLACIÓN EN SITUACIÓN DE EMERGENCIA
Sistema para el Desarrollo Integral de la Familia	PROGRAMA DE ATENCIÓN AL ADULTO MAYOR
Sistema para el Desarrollo Integral de la Familia	PROGRAMA PARA EL DESARROLLO DEL TALENTO DE JÓVENES
Sistema para el Desarrollo Integral de la Familia	PROGRAMA PARA LA ATENCIÓN Y PREVENCIÓN AL TRABAJO INFANTIL

Sistema para el Desarrollo Integral de la Familia	SERVICIOS DE REHABILITACIÓN Y ATENCIÓN A PERSONAS CON DISCAPACIDAD
Sistema para el Desarrollo Integral de la Familia	TALLER DE SENSIBILIZACIÓN
Sistema para el Desarrollo Integral de la Familia	TALLERES PRODUCTIVOS PARA PERSONAS CON DISCAPACIDAD INTELECTUAL
Sistema para el Desarrollo Integral de la Familia	TRANSPORTE SEGURO ADAPTADO
Sistema para el Desarrollo Integral de la Familia	VOLUNTARIADO DE SUPERACIÓN
Sistema para el Desarrollo Integral de la Familia	CIRUGÍAS DEL PROGRAMA CHRISTUS MUGUERZA
Tribunal de Arbitraje	PROCEDIMIENTO ANTE EL TRIBUNAL DE ARBITRAJE PARA LOS TRABAJADORES AL SERVICIO DEL MUNICIPIO DE MONTERREY

**Administración Pública Paramunicipal:** Instituto de las Mujeres Regias, Instituto de la Juventud Regia, Instituto Municipal de Planeación Urbana y Convivencia de Monterrey, Fideicomiso Distrito Tec y Fideicomiso de Mantenimiento Monterrey:

Instituto Municipal de las Mujeres Regias	ACTIVIDADES CÍVICAS, CULTURALES Y/O SOCIALES
Instituto Municipal de las Mujeres Regias	ASESORÍA Y ATENCIÓN
Instituto Municipal de las Mujeres Regias	BRIGADAS DE SALUD
Instituto Municipal de las Mujeres Regias	CAPACITACIÓN
Instituto Municipal de las Mujeres Regias	PROGRAMAS Y PROYECTOS DE PREVENCIÓN DE TRANSVERSALIDAD DE PERSPECTIVA DE GÉNERO
Instituto Municipal de las Mujeres Regias	PROGRAMAS Y PROYECTOS DE PREVENCIÓN DE LA VIOLENCIA CONTRA LAS MUJERES EN RAZÓN DE GÉNERO
Instituto de la Juventud Regia	ACOMPañAMIENTO ACADÉMICO
Instituto de la Juventud Regia	ASESORÍAS UANL
Instituto de la Juventud Regia	BANQUETERAS
Instituto de la Juventud Regia	BECAS
Instituto de la Juventud Regia	BOOTCAMP DE EMPRENDIMIENTO
Instituto de la Juventud Regia	BRIGADAS INJURE
Instituto de la Juventud Regia	CÁELE CON IDEAS
Instituto de la Juventud Regia	COLOR EN LAS CALLES
Instituto de la Juventud Regia	CONFERENCIAS POTENCIA JOVEN
Instituto de la Juventud Regia	CULTURA FISCA Y DEPORTE PREVENTIVO
Instituto de la Juventud Regia	CURSOS ICET





Instituto de la Juventud Regia	EMPRENDE A LO REGIO
Instituto de la Juventud Regia	ENSAMBLE CULTURAL
Instituto de la Juventud Regia	ENTRE MANOS NOS HABLAMOS
Instituto de la Juventud Regia	INJURED
Instituto de la Juventud Regia	INJUREFEST
Instituto de la Juventud Regia	JÁLATE A MADRID
Instituto de la Juventud Regia	JÓVENES POR LA INNOVACIÓN
Instituto de la Juventud Regia	JUVENTUD(ES) MONTERREY
Instituto de la Juventud Regia	JUVENTUDES SANAS
Instituto de la Juventud Regia	NÚTRETE A LO REGIO
Instituto de la Juventud Regia	POTENCIA JOVEN
Instituto de la Juventud Regia	PRIMER EMPLEO Y EMPRENDIMIENTO
Instituto de la Juventud Regia	PROYECTORES
Instituto de la Juventud Regia	REDES SOCIALES
Instituto de la Juventud Regia	REURBANIZARTE
Instituto de la Juventud Regia	TERAPIA DE A GRAPA
Instituto de la Juventud Regia	SISTEMA DE CÁMARAS DE SEGURIDAD
Instituto de la Juventud Regia	PROGRAMA DE TUTORÍAS ACADÉMICAS
Instituto de la Juventud Regia	ENCUESTA DE SATISFACCIÓN INJURE
Instituto Municipal de Planeación Urbana y Convivencia de Monterrey.	ASESORÍA TÉCNICA
Instituto Municipal de Planeación Urbana y Convivencia de Monterrey.	CÁMARAS DEL SISTEMA DE SEGURIDAD
Instituto Municipal de Planeación Urbana y Convivencia de Monterrey.	EXPEDIENTE LABORAL
Instituto Municipal de Planeación Urbana y Convivencia de Monterrey.	EXPEDIENTE DE PRESTADORES DE SERVICIO SOCIAL Y PRÁCTICAS PROFESIONALES
Instituto Municipal de Planeación Urbana y Convivencia de Monterrey.	ENCUESTAS
Instituto Municipal de Planeación Urbana y Convivencia de Monterrey.	EVENTOS DEL IMPLANC
Fideicomiso Distrito Tec	COMPRA DE BASES PARA PARTICIPAR EN LAS LICITACIONES
Fideicomiso Distrito Tec	EXPEDIENTE LABORAL
Fideicomiso de Mantenimientos (antes FIDEGRAN)	EXPEDIENTE LABORAL



Fideicomiso de Mantenimientos (antes FIDEGRAN)	FORMATO DE PAGO A CONTRATISTAS/PROVEEDORES
Fideicomiso de Mantenimientos (antes FIDEGRAN)	SOLICITUDES DE ACCESO A LA INFORMACIÓN
Fideicomiso de Mantenimientos (antes FIDEGRAN)	SOLICITUDES DE EJERCICIO DE DERECHOS ARCO

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

<https://www.monterrey.gob.mx/transparencia/Oficial /Inventario BD de Tratamiento de DP de Monterrey.html>

## 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 Centralizada y Paramunicipal, 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 Monterrey, 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 posea 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 Monterrey, 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 DT sobre los cambios que sufran sus trámites o sistemas de tratamiento de datos personales, los riesgos y las vulneraciones que surjan en el tratamiento de los datos personales, las 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 envío 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.

**III. ANÁLISIS DE RIESGOS:**

El análisis de riesgo tiene como objetivo alinear la protección de los datos personales que se traten en el Municipio de Monterrey, 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 Monterrey, los cuales han de ser protegidos, pues se pretende garantizar el servicio público que se otorga, por lo que debe de identificarse 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 impacto:





Nivel de Impacto	Descripción del impacto al presentar vulneración a los tratamientos de datos personales
Muy significativo	<p>Afecta al ejercicio de derechos fundamentales y libertades públicas establecidos en la Constitución, y sus consecuencias son irreversibles.</p> <p>Las consecuencias están relacionadas con categorías especiales de datos o relativos a infracciones penales, y es irreversible.</p> <p>Causa un daño social significativo, como la discriminación, y es irreversible.</p> <p>Afecta a interesados en situación de especial vulnerabilidad, en particular niños, y de forma irreversible.</p> <p>Causa pérdidas morales o materiales significativas e irreversibles.</p>
Significativo	<p>Los casos anteriores cuando los efectos son reversibles.</p> <p>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.</p> <p>Se produce o puede producirse usurpación de la identidad de los interesados.</p> <p>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.</p> <p>Existe un perjuicio social para los interesados o determinados colectivos de interesados.</p>
Limitado	<p>Pérdida 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.</p> <p>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.</p>
Muy limitado	<p>En el caso anterior, cuando todos los efectos son reversibles.</p>

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 vulneración 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 auditorías/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 auditorías 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.
<b>Documentos Personales:</b> <ul style="list-style-type: none"> <li>• Correos electrónicos</li> <li>• Actas de Nacimiento</li> <li>• Curp</li> <li>• Identificaciones</li> <li>• Documentos académicos</li> <li>• Documentos patrimoniales</li> <li>• Entre otros.</li> </ul>	Medio
<b>Aspectos personales:</b> <ul style="list-style-type: none"> <li>• Personas o grupos con los que se relaciona</li> <li>• Temperamento</li> <li>• Carácter</li> <li>• Inteligencia</li> <li>• Roles sociales</li> <li>• Capacidad de adaptación</li> <li>• Tolerancia al riesgo</li> </ul>	Alto





<ul style="list-style-type: none"><li>• Gustos/preferencias de contenidos audiovisuales (televisión interactiva, plataformas de contenidos, redes sociales, ...)</li><li>• Cuidado de salud</li><li>• Culturales (lectura, música, arte, ...)</li><li>• Pertenencia y actividades en asociaciones sociales y culturales</li><li>• Entre otros</li></ul>	
<p>Preferencias de consumo, hábitos, gustos, necesidades, etc. que no permitan inferir informaciones relacionadas con categorías especiales de datos:</p> <ul style="list-style-type: none"><li>• Preferencias de consumo: categoría de comercio, tipo de establecimiento; tipo de productos; etc.</li><li>• Hábitos de consumo</li><li>• Preferencias de contenidos audiovisuales en diferentes medios (televisión interactiva, plataformas de contenidos, redes sociales, ...)</li><li>• Preferencias de ocio (deportes, restaurantes, museos, teatros, música, etc.)</li><li>• Entre otros</li></ul>	Bajo
<p>Rendimiento laboral:</p> <ul style="list-style-type: none"><li>• Control de acceso al lugar de trabajo</li><li>• Grabación de imágenes en zonas de acceso o en oficinas</li><li>• Grabación de audio en zonas de acceso o en oficinas.</li><li>• Monitorización de los equipos de los empleados</li><li>• Inferencia del rendimiento a través de indicadores (Productividad y calidad del trabajo, Eficiencia, Formación adquirida, objetivos conseguidos)</li><li>• Entre otros</li></ul>	Medio
<p>Situación económica:</p> <ul style="list-style-type: none"><li>• Renta personal</li><li>• Ingresos mensuales</li><li>• Patrimonio (bienes muebles/inmuebles)</li><li>• Situación laboral</li><li>• Entre otros.</li></ul>	Medio
<p>Estado financiero:</p> <ul style="list-style-type: none"><li>• Solvencia financiera</li><li>• Pasivos (gastos en alimentación, vivienda, educación, salud, impuestos, pagos de créditos, tarjetas de crédito o gastos personales, etc.;</li><li>• Nivel de deuda (Préstamos personales, hipotecas)</li><li>• Ingresos.</li><li>• Entre otros.</li></ul>	Muy Alto
<p>Información Bancaria:</p> <ul style="list-style-type: none"><li>• Cuentas bancarias.</li><li>• Tarjetas.</li><li>• Entre otros.</li></ul>	Muy Alto
<p>Datos de comportamiento de empleados:</p> <ul style="list-style-type: none"><li>• Fiabilidad de la persona</li></ul>	Medio



<ul style="list-style-type: none"><li>• Hábitos y valores que facilitan la convivencia</li><li>• Hábitos y valores que facilitan el trabajo y el estudio</li><li>• Hábitos y valores que influyen en el bienestar personal, laboral y familiar</li><li>• Hábitos y valores que influyen en el compromiso con las personas y con la sociedad</li><li>• Estabilidad laboral.</li><li>• Antecedentes de comportamiento.</li><li>• Entre otra información.</li></ul>	
<b>Datos de localización:</b> <ul style="list-style-type: none"><li>• Registro de desplazamientos</li><li>• Registro de lugares habituales</li><li>• Registro de rutinas en base a localización</li><li>• Registro de lugares habituales</li></ul>	Medio
<b>Datos de Salud:</b> <ul style="list-style-type: none"><li>• Historia clínica</li><li>• Informes de salud</li><li>• Informes de baja laboral por motivos de salud para el Servicio de Prevención de Riesgos Laborales</li><li>• Recetas médicas</li><li>• Datos relativos a salud física</li><li>• Datos relativos a salud mental</li><li>• Datos relativos a prestación de servicios de atención sanitaria</li><li>• Documentos relativos a procesos asistenciales del paciente (incluida identificación de médicos y demás profesionales que han intervenido)</li><li>• Cualquier información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente.</li><li>• Datos Genéticos</li></ul>	Alto
<b>Datos biométricos:</b> <ul style="list-style-type: none"><li>• Huella dactilar</li><li>• Facciones rostro</li><li>• Iris</li><li>• Venas de la palma de la mano</li><li>• Voz</li><li>• Oreja</li><li>• Gestos</li><li>• Modo de andar</li><li>• Descriptores corporales de cualquier índole</li><li>• Trazos (firma)</li></ul>	Alto
<b>Categorías especiales de datos o que permitan inferirlos:</b> <ul style="list-style-type: none"><li>• Origen étnico</li><li>• Origen racial</li><li>• Opiniones políticas</li><li>• Convicciones religiosas</li><li>• Convicciones filosóficas</li></ul>	Alto





<ul style="list-style-type: none"> <li>• Afiliación sindical</li> <li>• Datos relativos a la salud</li> <li>• Datos relativos a la vida sexual</li> <li>• Datos relativos a las orientaciones sexuales</li> <li>• Entre otros.</li> </ul>	
Datos personales relativos a probables delitos e infracciones administrativas.	Muy Alto
<b>Metadatos:</b> <ul style="list-style-type: none"> <li>• Datos de tráfico de las comunicaciones electrónicas</li> <li>• Identificación de emisor y/o receptor en las comunicaciones</li> <li>• 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).</li> <li>• Entre otros.</li> </ul>	Medio
<b>Datos de Identificación:</b> <ul style="list-style-type: none"> <li>• Nombre</li> <li>• Estado Civil</li> <li>• Fecha de Nacimiento.</li> <li>• Nacionalidad</li> <li>• Lugar de nacimiento</li> <li>• Domicilio</li> <li>• Teléfono</li> <li>• Correo electrónico</li> <li>• Firma autógrafa</li> <li>• Firma electrónica</li> <li>• Edad</li> <li>• imagen</li> </ul>	Bajo

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

Categoría 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 algún 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 Monterrey, así como de sus Paramunicipales, 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 se precisará de acuerdo en la siguiente tabla:

Tipo de Dato	Nivel de Riesgo Inherente
Información financiera y Bancaria	Muy Alto
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 Monterrey 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 cómo 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

El 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 Categoría de Datos.	Nivel de Impacto	Vulnerabilidad	Número de Titulares	Nivel de Riesgo
<b>ACTIVIDAD</b>				
<b>Perfilación:</b> <ul style="list-style-type: none"> <li>• Creación de perfiles</li> <li>• Uso de perfiles</li> <li>• Clasificación de individuos</li> <li>• Orientación de productos/servicios a individuos o grupos</li> <li>• Análisis comportamental (evaluación y calificación de emociones, estados de ánimo, hábitos, preferencias, etc.)</li> </ul> Entre otros que pudieran derivar.	Alto	Acceso no autorizado al rastro digital de las y los usuarios, vulnerando la información de acuerdo al comportamiento de que se trate o finalidad de la actividad.	+ 5,000	3
<b>Predicción:</b> <ul style="list-style-type: none"> <li>• Inferencia de nuevos datos personales.</li> <li>• Modificaciones.</li> <li>• Entre otros que pudieran derivar.</li> </ul>	Alto	Vulneración de registros de todos los datos personales de servidores públicos y usuarios que han otorgado su consentimiento para automatizar sus datos.	- 500	1
<b>Control de los Servidores Públicos:</b> <ul style="list-style-type: none"> <li>• Evaluación del empleado</li> <li>• Observación del puesto de trabajo</li> <li>• Monitorización del puesto de trabajo</li> <li>• Grabación de imágenes en ámbito laboral</li> <li>• Grabación de audio en ámbito laboral</li> <li>• Monitorización por medio de imágenes en ámbito laboral</li> <li>• Monitorización por medio de sonido en ámbito laboral</li> <li>• Tiempo invertido en realizar tareas</li> <li>• Monitorización y control de correo electrónico</li> <li>• Control de Asistencia.</li> <li>• Control de uso de teléfono</li> </ul> Entre otros que pudieran derivar.	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
<b>Control del Acceso a Internet:</b> <ul style="list-style-type: none"> <li>• Análisis o evaluación de tiempos de uso de Internet</li> <li>• Control de permisos para actividades de navegación en Internet</li> <li>• Análisis o evaluación de alarmas sobre navegación a sitios específicos en Internet</li> <li>• Análisis o evaluación de alarmas sobre navegación a contenidos específicos en Internet</li> </ul> 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 los permisos para autorizaciones en la red, lo cual no constituye el ingreso a los servidores donde se almacena información.	+5,000	2
<b>Observación:</b> <ul style="list-style-type: none"> <li>• Vigilancia mediante imágenes</li> <li>• Vigilancia mediante sonidos</li> </ul>	Alto	Vulneración a la video vigilancia de los edificios y centros físicos del Municipio, así como de las	+ 50,000	3





Documento de Seguridad para la Protección de los Datos Personales

<ul style="list-style-type: none"> <li>• Vigilancia de comunicaciones</li> <li>• Vigilancia de Internet</li> </ul> <p>Entre otros que pudieran derivar.</p>		comunicaciones oficiales e información en la nube.		
<p>Monitorización:</p> <ul style="list-style-type: none"> <li>• Control mediante imágenes</li> <li>• Control mediante sonidos</li> <li>• Control de comunicaciones</li> <li>• Control de transmisiones</li> <li>• Control de Internet</li> </ul> <p>Entre otros que pudieran derivar.</p>	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
<p>Supervisión:</p> <ul style="list-style-type: none"> <li>• Control</li> <li>• Análisis mediante imágenes</li> <li>• Análisis mediante sonidos</li> <li>• Análisis de comunicaciones</li> <li>• Análisis de transmisiones</li> <li>• Análisis de Internet</li> <li>• Control de tráfico rodado</li> </ul> <p>Entre otros que pudieran derivar.</p>	Alto	Acceso no autorizado a la información relativa a la supervisión de actividades de las y los servidores públicos.	+ 50,000	3
<p>Control físico de acceso:</p> <ul style="list-style-type: none"> <li>• Control de acceso a las instalaciones</li> <li>• Control de acceso a eventos</li> <li>• Control de acceso a instalaciones deportivas</li> <li>• Control de acceso a las áreas en específico.</li> </ul> <p>Entre otros que pudieran derivar.</p>	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		
<p>Decidir sobre o impedir el ejercicio de derechos fundamentales:</p> <ul style="list-style-type: none"> <li>• Derecho a la igualdad</li> <li>• Derecho a la no discriminación</li> <li>• Derecho a la vida y a la integridad física</li> <li>• Derecho a la libertad religiosa</li> <li>• Derecho a la libertad personal</li> <li>• Derecho al patrimonio</li> <li>• Derecho a la intimidad personal y familiar</li> <li>• Derecho a la propia imagen</li> <li>• Derecho a la libertad de expresión e información</li> <li>• Derecho a la libertad de cátedra</li> <li>• Derecho a la libertad de reunión</li> <li>• Derecho a la libertad de asociación</li> <li>• Derecho al libre acceso a cargos y funciones públicas en condiciones de igualdad</li> <li>• Derecho a la legalidad penal</li> <li>• Derecho a la educación</li> <li>• Derecho a la libertad sindical</li> </ul>	Alto	Vulneración a los procesos que se llevan a cabo en el Municipio o sus dependencias paramunicipales, referentes a solicitudes, servicios, procedimientos, dudas o quejas, así como cualquiera que se encuentre dentro de las facultades del Municipio de Monterrey.	+ 500,000	3



Documento de Seguridad para la Protección de los Datos Personales

<ul style="list-style-type: none"> <li>• Derecho de petición</li> <li>Otros derechos o libertades consagradas en la Constitución Política de los Estados Unidos Mexicanos.</li> </ul>				
Decidir sobre el control del interesado de sus datos personales: <ul style="list-style-type: none"> <li>• Derecho de acceso</li> <li>• Derecho de rectificación</li> <li>• Derecho de oposición</li> <li>• Derecho de Cancelación</li> <li>Derecho a la portabilidad</li> </ul>	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 Monterrey y/o sus Paramunicipales.	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 o beneficiarias a un apoyo.	+ 500	4
Servicios o tramites que tengan efectos jurídicos sobre las personas	Alto	Anticipación a las resoluciones y manipulación o sustracción de personas y/o trámites.	+ 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
<b>DATOS PERSONALES</b>				
Documentos Personales: <ul style="list-style-type: none"> <li>• Correos electrónicos</li> <li>• Actas de Nacimiento</li> <li>• Curp</li> <li>• identificaciones</li> <li>• Documentos académicos</li> <li>• Documentos patrimoniales</li> <li>Entre otros.</li> </ul>	Medio	Vulneración a la información personal de identificación, académica y patrimonial de usuarios y servidores públicos.	+ 500,000	3
Aspectos personales: <ul style="list-style-type: none"> <li>• Personas o grupos con los que se relaciona</li> <li>• Temperamento</li> <li>• Carácter</li> <li>• Inteligencia</li> <li>• Roles sociales</li> <li>• Capacidad de adaptación</li> <li>• Tolerancia al riesgo</li> <li>• Gustos/preferencias de contenidos audiovisuales (televisión interactiva,</li> </ul>	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





<p>plataformas de contenidos, redes sociales, ...)</p> <ul style="list-style-type: none"> <li>• Cuidado de salud</li> <li>• Culturales (lectura, música, arte, ...)</li> <li>• Pertenencia y actividades en asociaciones sociales y culturales</li> </ul> <p>Entre otros</p>				
<p>Preferencias de consumo, hábitos, gustos, necesidades, etc. que no permitan inferir informaciones relacionadas con categorías especiales de datos:</p> <ul style="list-style-type: none"> <li>• Preferencias de consumo: categoría de comercio, tipo de establecimiento; tipo de productos; etc.</li> <li>• Hábitos de consumo</li> <li>• Preferencias de contenidos audiovisuales en diferentes medios (televisión interactiva, plataformas de contenidos, redes sociales, ...)</li> <li>• Preferencias de ocio (deportes, restaurantes, museos, teatros, música, etc.)</li> </ul> <p>Entre otros</p>	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
<p>Rendimiento laboral:</p> <ul style="list-style-type: none"> <li>• Control de acceso al lugar de trabajo</li> <li>• Grabación de imágenes en zonas de acceso o en oficinas</li> <li>• Grabación de audio en zonas de acceso o en oficinas.</li> <li>• Monitorización de los equipos de los empleados</li> <li>• Inferencia del rendimiento a través de indicadores (Productividad y calidad del trabajo, Eficiencia, Formación adquirida, objetivos conseguidos)</li> </ul> <p>Entre otros</p>	Medio	Vulneración al modo de trabajo de las personas, así como a la privacidad en sus centros de trabajo.	+ 5,000	2
<p>Situación económica:</p> <ul style="list-style-type: none"> <li>• Renta personal</li> <li>• Ingresos mensuales</li> <li>• Patrimonio (bienes muebles/inmuebles)</li> <li>• Situación laboral</li> </ul> <p>Entre otros.</p>	Medio	Puede ocasionar discriminación, o bien ser objetivos para fraudes o extorciones.	+ 50,000	3
<p>Estado financiero:</p> <ul style="list-style-type: none"> <li>• Solvencia financiera</li> <li>• Pasivos (gastos en alimentación, vivienda, educación, salud, impuestos, pagos de créditos, tarjetas de crédito o gastos personales, etc.;</li> </ul>	Muy Alto	Puede ocasionar discriminación, o bien ser objetivos para fraudes o extorciones.	+ 5,000	5



Documento de Seguridad para la Protección de los Datos Personales

<ul style="list-style-type: none"> <li>• Nivel de deuda (Préstamos personales, hipotecas)</li> <li>• Ingresos.</li> </ul> <p>Entre otros.</p>				
<p>Información Bancaria:</p> <ul style="list-style-type: none"> <li>• Cuentas bancarias.</li> <li>• Tarjetas.</li> </ul> <p>Entre otros.</p>	Muy Alto	Puede ocasionar discriminación, o bien ser objetivos para fraudes o extorsiones.	+ 5,000	5
<p>Datos de comportamiento de empleados:</p> <ul style="list-style-type: none"> <li>• Fiabilidad de la persona</li> <li>• Hábitos y valores que facilitan la convivencia</li> <li>• Hábitos y valores que facilitan el trabajo y el estudio</li> <li>• Hábitos y valores que influyen en el bienestar personal, laboral y familiar</li> <li>• Hábitos y valores que influyen en el compromiso con las personas y con la sociedad</li> <li>• Estabilidad laboral.</li> <li>• Antecedentes de comportamiento.</li> </ul> <p>Entre otra información.</p>	Medio	Pueden ser objetos de algún tipo de distinción o de ataques sociales por su comportamiento laboral y académico.	+ 5,000	2
<p>Datos de localización:</p> <ul style="list-style-type: none"> <li>• Registro de desplazamientos</li> <li>• Registro de lugares habituales</li> <li>• Registro de rutinas en base a localización</li> </ul> <p>Registro de lugares habituales</p>	Medio	Puede ser objeto de ataques, fraudes o extorsiones 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
<p>Datos de Salud:</p> <ul style="list-style-type: none"> <li>• Historia clínica</li> <li>• Informes de salud</li> <li>• Informes de baja laboral por motivos de salud para el Servicio de Prevención de Riesgos Laborales</li> <li>• Recetas médicas</li> <li>• Datos relativos a salud física</li> <li>• Datos relativos a salud mental</li> <li>• Datos de la prestación de servicios de atención sanitaria</li> <li>• Documentos relativos a procesos asistenciales del paciente (incluida identificación de médicos y demás profesionales que han intervenido)</li> <li>• Cualquier información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente.</li> <li>• Datos Genéticos</li> </ul>	Alto	Pueden ser objeto de ataques a la privacidad personal, discriminación, manipulación, o perjuicio moral.	+ 5,000	3
<p>Datos biométricos:</p> <ul style="list-style-type: none"> <li>• Huella dactilar</li> <li>• Facciones rostro, Iris</li> <li>• Venas de la palma de la mano</li> </ul>	Alto	Vulnera los datos de autenticación, lo cual puede traer para las personas perjuicio económico, patrimonial y laboral.	+ 5,000	3





<ul style="list-style-type: none"> <li>• Voz, Oreja, Gestos</li> <li>• Modo de andar</li> <li>• Descriptores corporales de cualquier índole</li> </ul> <p>Trazos (firma)</p>				
<p>Categorías especiales de datos o que permitan inferirlos:</p> <ul style="list-style-type: none"> <li>• Origen étnico</li> <li>• Origen racial</li> <li>• Opiniones políticas</li> <li>• Convicciones religiosas</li> <li>• Convicciones filosóficas</li> <li>• Afiliación sindical</li> <li>• Datos relativos a la salud</li> <li>• Datos de la vida sexual</li> <li>• Datos relativos a las orientaciones sexuales</li> </ul> <p>Entre otros.</p>	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 a 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
<p>Metadatos:</p> <ul style="list-style-type: none"> <li>• Datos de tráfico de las comunicaciones electrónicas</li> <li>• Identificación de emisor y/o receptor en las comunicaciones</li> <li>• 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).</li> </ul> <p>Entre otros.</p>	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
<p>Datos de Identificación:</p> <ul style="list-style-type: none"> <li>• Nombre</li> <li>• Estado Civil</li> <li>• Fecha de Nacimiento.</li> <li>• Nacionalidad</li> <li>• Lugar de nacimiento</li> <li>• Domicilio</li> <li>• Teléfono</li> <li>• Correo electrónico</li> <li>• Firma autógrafa</li> <li>• Firma electrónica</li> <li>• Edad</li> </ul> <p>imagen</p>	Bajo	Acceso no autorizado a información del personal del Municipio y sus Paramunicipales, o bien a la información de las personas usuarias, vulnerándose su información personal de identificación y contacto.	+ 500,000	1

Categoría de Titular / Factor de riesgo				
Menores de 14 años	Muy Alto	Vulneración a información de menores de edad.	+ 50,000	5
Víctimas de violencia de género	Muy Alto	Identidad de las víctimas lo cual las pone en un riesgo de daño físico, moral y social.	+ 5,000	4
Menores dependientes de sujetos vulnerables	Muy Alto	Se pondría en riesgo la identidad de estas personas así como las necesidades, pudiendo ser víctimas de algún delito.	+ 500	4
Personas bajo guardia y custodia de víctimas de violencia de género	Muy Alto	Identidad de menores en situaciones vulnerables, afectando su moral y su integridad física.	+ 500	4
Mayores con algún grado de discapacidad	Muy Alto	Vulneración de su información personal sensible.	+ 5,000	4
Personas mayores	Alto	La divulgación de su información sin su consentimiento podría hacerlos víctimas de algún fraude.	+ 50,000	3
Personas con enfermedades mentales	Muy Alto	Se podría vulnerar su información personal sensible y podrían ser víctimas de discriminación.	+ 5,000	4
Discapacitados	Muy Alto	Se podría vulnerar su información personal sensible y podrían ser víctimas de discriminación.	+ 5,000	4
Personas que acceden a servicios sociales	Medio	Podrían ser excluidos de ciertos lugares y/o grupos sociales.	+ 50,000	3
Sujetos en riesgo de exclusión social	Muy Alto	Podrían ser víctimas de discriminación	+ 500	4
Solicitantes de asilo	Alto	La divulgación de su información sin su consentimiento podría hacerlos víctimas de algún fraude.	+ 5,000	3
Pacientes	Alto	Se podría vulnerar su información personal sensible y podrían ser víctimas de discriminación.	+ 5,000	3
Personas vulnerables: • En situación de especial vulnerabilidad • Existe un desequilibrio entre la posición del titular y del responsable	Muy Alto	Se podría vulnerar su información personal sensible y podrían ser víctimas de discriminación.	+ 500	4

#### IV. ANÁLISIS DE BRECHA:

Para realizar el análisis de brecha, la Dirección de Transparencia de la Contraloría Municipal de Monterrey, elaboró y aplicó un cuestionario 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 Centralizada y las Entidades Paramunicipales.

Una vez identificados los posibles riesgos a los que el Municipio de Monterrey se encuentra susceptible de enfrentar, se formula el presente análisis de brecha, utilizando como base el siguiente cuestionario de Medidas de Seguridad:



**A) Medidas de Seguridad basadas en la cultura del personal:**

- A.1. ¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?
- A.2. ¿Tienes mecanismos para eliminar de manera segura la información?
- A.3. ¿Has establecido y documentado los compromisos respecto a la protección de datos?
- A.4. ¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?
- A.5. ¿Realizas respaldos periódicos de los datos personales?

**B) Medidas de seguridad en el entorno de trabajo físico:**

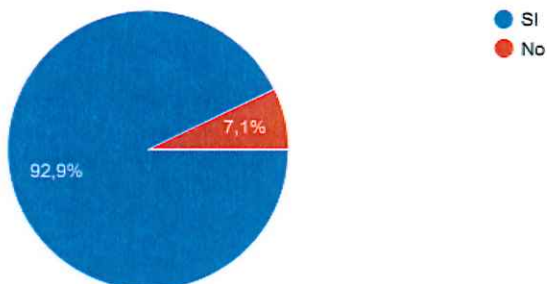
- B.1. ¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?
- B.2. ¿Tienes medidas de seguridad para evitar el robo?
- B.3. ¿Cuidas los movimientos de información en entornos de trabajo físico?

**C) Medidas de seguridad en el entorno de trabajo digital:**

- C.1. ¿Realizas actualizaciones al equipo de cómputo?
- C.2. ¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?
- C.3. ¿Tienes medidas de seguridad para navegar en entornos digitales?
- C.4. ¿Cuidas el movimiento de información en entornos de trabajo digitales?

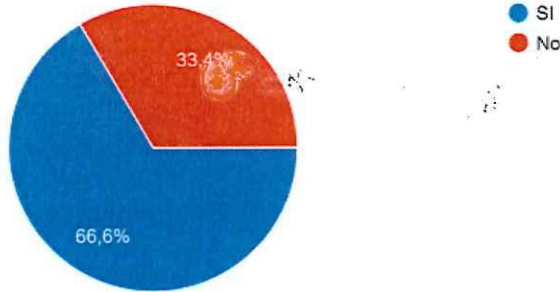
A continuación, se presentan los resultados de las encuestas aplicadas a las personas servidoras públicas del Municipio de Monterrey, de acuerdo a las medidas que implementan dentro de sus labores cotidianas:

- A.1. ¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?  
(por ejemplo, en el escritorio o en alguna otra área...trada toda la documentación con la que se trabaja)

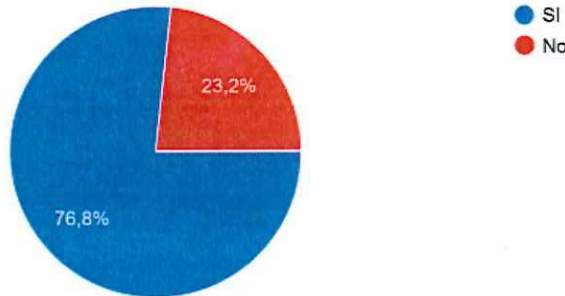




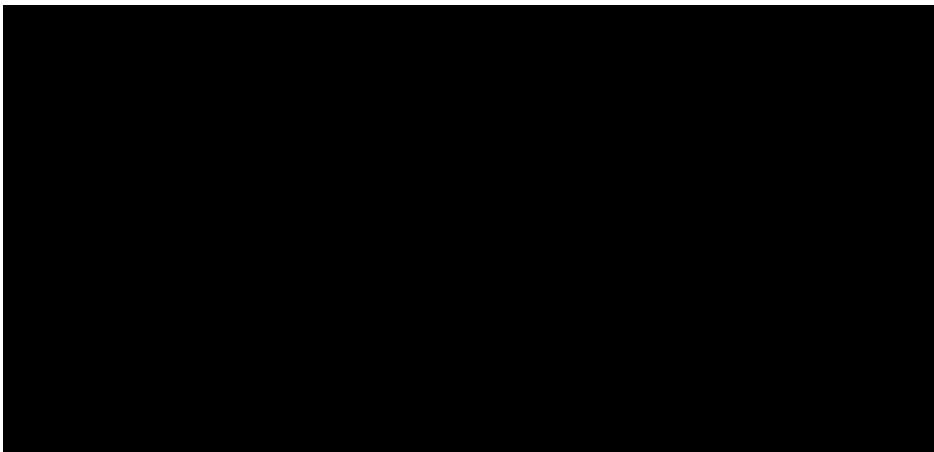
A.2. ¿Tienes mecanismos para eliminar de manera segura la información? (borrado de archivos electrónicos, trituración de hojas que contienen datos personales, etc)



A.3. ¿Has establecido y documentado los compromisos respecto a la protección de datos? (conoces de la materia y organizas la información ...o a los datos que manejas en tus labores diarias)



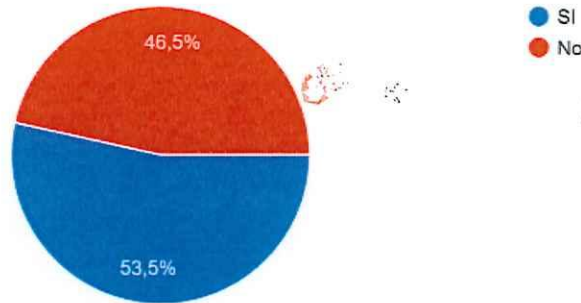
A.4. ¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales? (dentro del área, se les ha informado ...eso no autorizado a los equipos de cómputo, etc.)



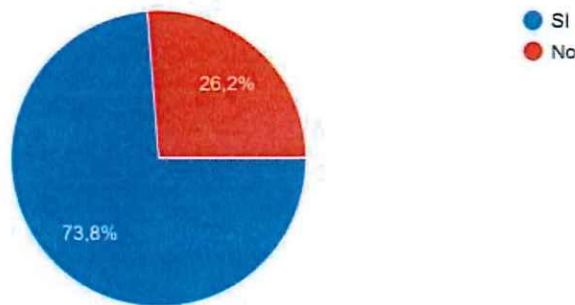




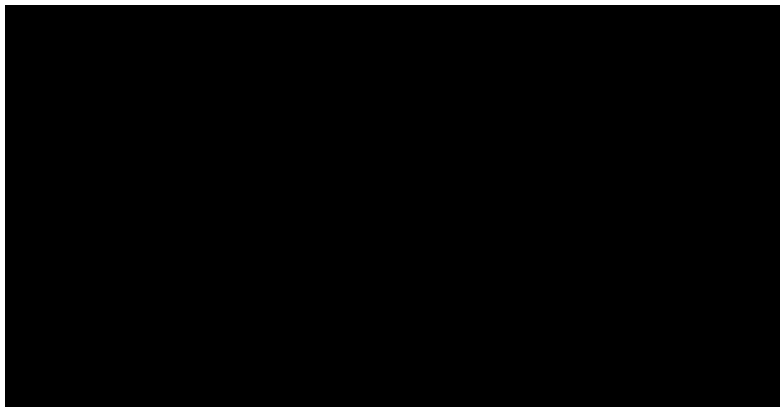
A.5. ¿Realizas Respaldos periódicos de los datos personales? (haces respaldo de la información que manejas en la nube, en USB o disco duro externo)



B.1. ¿Tienes medidas de seguridad para acceder al entorno de trabajo físico? (filtro de seguridad en entrada, acceso restringido al público en general o a personal que no es del área)

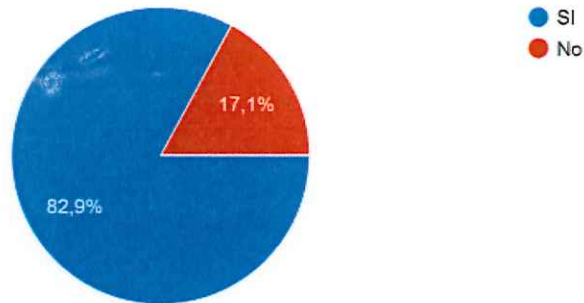


B.2. ¿Tienes medidas de seguridad para evitar el robo? (archivero con llave, cámaras de seguridad, personal de seguridad)

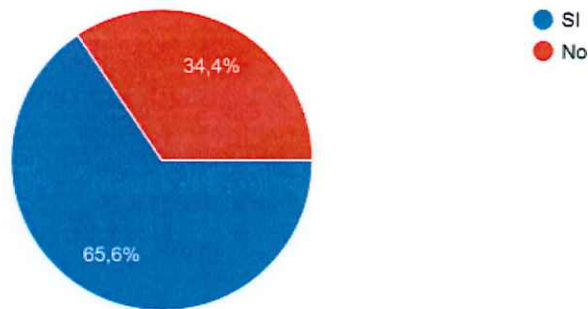




B.3. ¿Cuidas los movimientos de información en entornos de trabajo físico? (que solamente tenga acceso a la información personal autorizado y que ...fuera de la Coordinación, Dirección o Secretaría)



C.1. ¿Realizas actualizaciones al equipo de cómputo? (Te aseguras que el personal de sistemas realice las actualizaciones necesarias a tu equipo)









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

1.- ¿Se tienen medidas de seguridad físicas, técnicas y administrativas para salvaguardar la información del servidor físico principal? [Redacted]

2.- ¿Se tiene un respaldo de toda la información en algún medio físico? [Redacted]

3.- ¿Se tiene Respaldo de toda la información en la nube? [Redacted]

4.- ¿Cuenta con medidas de contingencia ante ciberataques? - [Redacted]

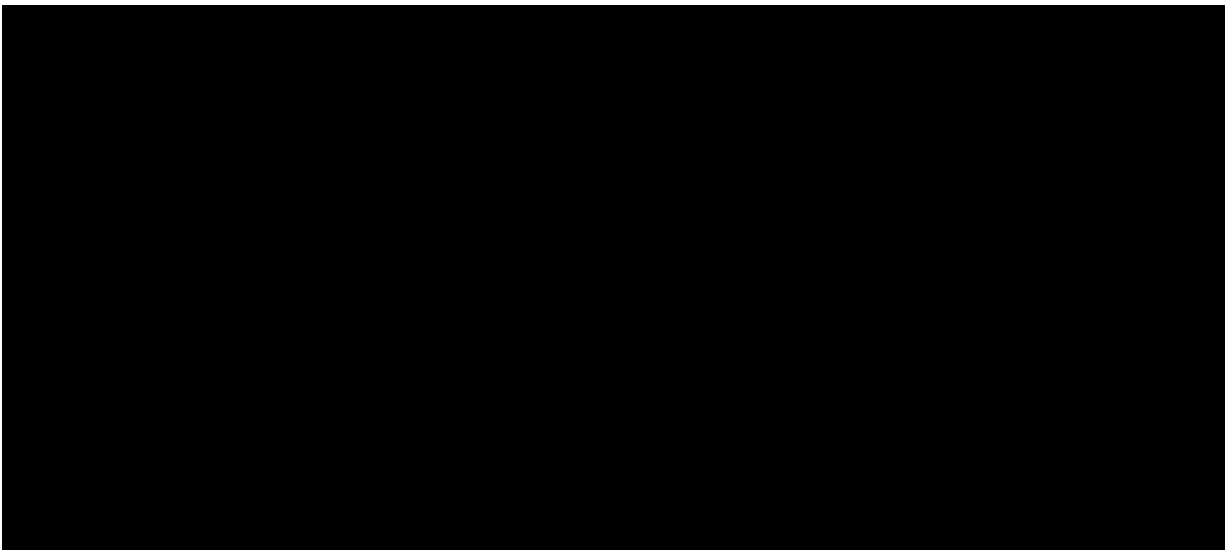
5.- ¿Revisa periódicamente el software instalado en los equipos de cómputo? - [Redacted]

6.- ¿Revisa la configuración de la seguridad de todos los equipos de cómputo? - [Redacted]

7.- 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:

[Large redacted area]





En tal sentido, se tiene que el sistema de seguridad informática es acorde a las necesidades del Municipio de Monterrey, sin embargo, en cuanto a las actividades de las y los 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 Monterrey y sus Paramunicipales, 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 Centralizada y las Paramunicipales, 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 Centralizada y las Dependencias Paramunicipales, realizarán para 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:

1. 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 Monterrey.



2. 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 Monterrey y sus Paramunicipales, 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.
3. Enviar un comunicado electrónico al personal del Municipio de Monterrey y sus Entidades Paramunicipales en el cual se informará:
  - Los Lineamientos en materia de Protección de Datos Personales para los Sujetos Obligados del Municipio de Monterrey.
  - Los conceptos básicos de la Protección de Datos Personales.
  - Mejores prácticas para respaldar información
4. [Redacted]
5. [Redacted]
6. [Redacted]
7. [Redacted]
8. Mantener actualizados los avisos de privacidad e inventarios 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 ADMINISTRACIÓN PÚBLICA MUNICIPAL CENTRALIZADA Y LAS DEPENDENCIAS PARAMUNICIPALES DE MONTERREY.

#### Medidas de seguridad físicas y administrativas

Las Dependencias de la Administración Pública Municipal Centralizada y las Entidades Paramunicipales, 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:

- I. 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.
- II. Tener bajo llave o asegurados los archiveros, archivos, cajas y almacenes en donde se encuentre almacenada la información de datos personales.
- III. Evitar que se dejen descuidados o sin la atención debida documentos que contengan datos personales.
- IV. Establecer un plan de contingencia con protocolos de seguridad, que incluya, cuando menos, la 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.

- V. 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.
- VI. Implementar programas de capacitación en materia de protección de datos personales al interior del Municipio y sus Entidades Paramunicipales.

### Medidas de seguridad en el entorno

Las Dependencias de la Administración Pública Municipal Centralizada y las Entidades Paramunicipales, 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:

- I. Registrar a visitantes que accedan a instalaciones;
- II. Portar el gafete de visitante dentro de las instalaciones, por personas ajenas a la Administración Pública Municipal Centralizada y las Paramunicipales;
- III. Asegurar el retiro de pases de visita.
- IV. 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 Centralizada y Entidades Paramunicipales, deberán implementar como mínimo las siguientes medidas, para evitar daños, sustracciones o intromisiones no autorizadas:

- I. Registrar la información que corresponda en los tratamientos de Datos Personales y mantenerlos actualizados;
- II. Requerir el apoyo en tecnologías de información que sea necesario por parte de la Secretaría de Innovación y Gobierno Abierto para efectos del soporte informático requerido;
- III. 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;
- IV. 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 Centralizada y Paramunicipal.
- V. 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 Centralizada y las Entidades Paramunicipales, en coordinación con la Dirección General de Gobierno Digital y Soporte Tecnológico de la Secretaría de Innovación y Gobierno Abierto, implementará cuando menos las siguientes **medidas de seguridad en equipos computacionales que contengan documentos, archivos o sistemas de datos personales:**

- I. [Redacted]
- II. [Redacted]
- III. Limitar o restringir por completo el uso de internet en los equipos que se estime pertinente.
- IV. [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 Centralizada y Paramunicipal, el personal que labora en oficinas de partes de cada dependencia deberá registrar a las personas y previa identificación, darle el acceso correspondiente con una tarjeta de visitante.

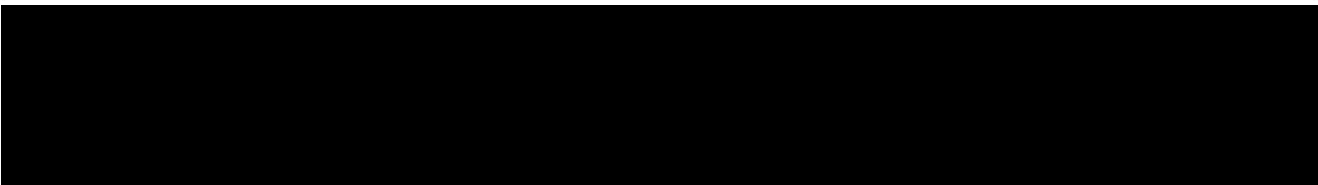
**Medidas de seguridad en caso de desastres naturales:**

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

**Medidas de seguridad con respecto a la infraestructura tecnológica:**

Con fundamento en el artículo 116 del Reglamento de la Administración Pública Municipal de Monterrey, la Secretaría de Innovación y Gobierno Abierto, a través de la Dirección General de Gobierno Digital y Soporte Tecnológico es la unidad administrativa encargada de las medidas de seguridad con respecto a:

- Amenazas externas en la red
- Antivirus
- Firewall
- Instalación de software no autorizado
- Servidores y sus copias de seguridad
- Copias de seguridad o respaldos de la Información de los servidores



T ^ á ä æ / ä ^ Ä ^ \* ^ ! ä ä ä Ä ^ ^ / ä [ { ] ! [ { ^ ö } Ä ä ö ( æ Ä / ä ä ä ^ • / Ä Ä Q + ! { ä ä ä } Ä ^ • ^ ! ç ä ä ä ä ^ / ä [ ] + ! { ä ä ä / ä [ ] Ä [ Ä ä ] ^ ^ • ç Ä } Ä | Ä ä ä ä [ | Ä H Ä ä ä ä ) Ä Ä ^ Ä ä ä ^ / ä ^ Ä / ä ä ] ä ä ^ ä ä Ä / ä ä ä ^ • [ Ä Ä | ä Q + ! { ä ä ä } Ä ä ä | ä ä ä ^ / ä • ä ä [ Ä ^ Ä ^ ^ ç [ Ä ^ 5 )





## 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 Monterrey, cuenta con el apoyo de la Dirección General de Gobierno Digital y Soporte Tecnológico de la Secretaría de Innovación y Gobierno Abierto, 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.

### Físicamente:

**1.-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.

**2.-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:

**1.-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 Centralizada y Paramunicipal, 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 Centralizada y Paramunicipal de Monterrey, 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.

Dado en el Comité de Transparencia de la Administración Pública Centralizada del Municipio de Monterrey, Nuevo León, a los 02-dos días del mes de mayo de 2023 dos mil veintitrés.

#### COMITÉ DE TRANSPARENCIA DE LA ADMINISTRACIÓN PÚBLICA CENTRALIZADA DEL MUNICIPIO DE MONTERREY

RÚBRICA  
JOSÉ ANTONIO GÓMEZ VILLARREAL  
PRESIDENTE DEL COMITÉ

RÚBRICA  
RAÚL ROBLES GÓMEZ  
SECRETARIO TÉCNICO DEL COMITÉ

RÚBRICA  
CECILIA ÁVILA PÉREZ  
VOCAL DEL COMITÉ