SAN NICOLÁS DE LOS GARZA GOBIERNO DE LA CIUDAD

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

Arturo B. de la Garza No. 1600 Colonia Valle Dorado, San Nicolás de los Garza, Nuevo León. Tels. 81581341
transparencia@sanicolas.gob.mx

CONTENIDO

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 San Nicolás de los Garza, 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, el Centro Integral de Transparencia y Protección de Datos Personales, 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 San Nicolás de los Garza, 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 libertades reconocidos en esta Constitución dentro del ámbito digital y serán plenamente aplicables en ese ámbito. Se promoverá, a atraves 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 la medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los daros 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 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

VI. 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 incumplimientode 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

Área administrativa: son las unidades que conforman la estructura orgánica del sujeto obligado, cuyos titulares de cada una de las áreas figuran como responsables del tratamiento de datos personales en particular.

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada e identificable, condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

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.

Hardware: es el conjunto de componentes físicos de los que está hecho el equipo.

Software: es la parte no física que hace referencia a un programa o conjunto de programas de cómputo que incluye datos, reglas e instrucciones para poder comunicarse con el ordenador y que hacen posible su funcionamiento.

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

Medidas de seguridad: 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: Políticas y procedimiento para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.

Nube: Modelo de provisión externa de servicios de computo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

Respaldo o Backup: Es una copia de la información que una organización 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.

Titular: Persona física a quien pertenecen los datos personales.

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado.

Tratamiento: De manera enunciativa mas no limitativa cualquier operación o conjunto de operaciones efectuadas mediante procedimiento manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de los datos personales.

Sistema de Datos Personales: Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso.

INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

En el presente documento, se estableció un inventario de datos personales y de los sistemas tratados por las dependencias que se encuentran en medios de almacenamiento físicos así como electrónicos.

Los mismos se presentan por áreas administrativas previstas en base al Reglamento Orgánico Municipal de San Nicolás de los Garza, Nuevo León, mismas que cuentan o pueden contar, dar tratamiento y, ser responsables o encargados de los datos personales. Descripción y estructura de las bases de datos o sistemas de tratamiento de datos personales. En la descripción de cada base o sistema de tratamiento de datos personales, se indica cuáles son los datos personales que se recaban, con que 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 actué a cuenta y nombre del Municipio de San Nicolás de los Garza, N.L y, el servidor público encargado de administrar la base o sistema de tratamiento de datos personales así como los subordinados que tienen acceso a las mismas, tal como se indica en la siguiente ilustración.

Área o dirección	Área administrativa del sujeto obligado que figura como responsable del tratamiento de datos personales
Base de datos o sistema de tratamiento	Denominación de la base o sistema de tratamiento de datos personales que utiliza el área administrativa del Municipio de San Nicolás de los Garza, N.L
Categoría de los datos personales	Datos de identificación y contacto, Datos sobre características físicas, Datos laborales, Datos académicos, Datos patrimoniales y/o financieros, Datos biométricos. etc.
Datos personales que se recaban	Todos aquellos datos en específico que recaba el área administrativa.

Finalidad para la cual se obtuvieron (especificar si es finalidad principal o secundaria)	Todo tratamiento de datos personales que efectué el responsable debe estar justificado por finalidades concretas, licitas, explicitas y legítimas, relacionadas con las atribuciones que normatividad aplicable les confiera. Finalidad principal: Dan origen y son necesarias para la relación jurídica. Finalidad secundaria: No son necesarias para la relación jurídica (publicidad, mercadotécnica)
Fundamento legal que faculta para el tratamiento	El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable les confiera.
Forma de obtención directa/indirectamente del titular medios físicos/electrónicos.	• Directamente del titular: *De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso. *Vía telefónica. * Por correo electrónico. * Por Internet o sistema informático. * Por escrito presentado directamente en las oficinas del sujeto obligado. * Por escrito enviado por mensajería. • Mediante una transferencia: * Quien transfiere los datos personales y para que fines. *Medios por los que se realiza la transferencia. • De una fuente de acceso público: *Las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales este concebido para facilitar información al público y este abierto a la consulta general; * Los directorios telefónicos en términos de la normativa específica; *Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa.

	* Los medias de comunicación social, y * Los registros públicos conforme a las disposiciones que resulten aplicables.
Medios de almacenamiento físicos/electrónicos	**Físico**: Todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún apartado que procese su contenido para examinar, modificar o almacenar datos personales, por ejemplo los expedientes de personal almacenados en un archivero. En este sentido hay que considerar cuantos especiales, muebles, cajones y cualquier espacio donde se guarden formatos físicos, o bien equipos de cómputo u otros medios de almacenamiento. **Electrónico**: Todo recurso al que se puede acceder solo mediante el uso de equipo de cómputo (cualquier dispositivo electrónico que permita el procesamiento de información por ejemplo, computadoras de escritorio, laptops, tabletas, teléfonos inteligentes, entre otros) que procese su contenido para examinar, modificar o almacenar los datos personales. Podemos considerar por ejemplo, discos duros (tanto propios del equipo de cómputo como los portátiles), memorias extraíbles como USB o C.D's, entre otros. También podemos contemplar como medio de almacenamiento electrónico, el uso de servicios de almacenamiento en línea.
Sitios de resguardo	Toda locación donde se resguarden los medios de almacenamiento, tanto físicos como electrónicos (ejemplo, casa, Municipio, instalaciones de un tercero).
Servidores públicos que tiene acceso a los sistemas de datos personales	Personal adscrito al Municipio de San Nicolás de los Garza, N.L. autorizado para llevar a cabo el tratamiento de datos personales.
Encargado	Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

Catálogo de sistemas de tratamiento o bases de datos personales.

SECRETARÍA DEL AYUNTAMIENTO

1. Dirección de Gobierno

1.1 Carta de Residencia, Identidad, Concubinato y Manifiesto
1.2 Recepción de documentos para Trámite de Cartilla Militar
1.3 Tramite de Pasaporte

2. Dirección de Inspección.

2.1 Captura de actas

3. Dirección de Bomberos y Protección Civil.

3.1 Solicitud de Inspección / Constancia de Servicio

4. Sistema de Justicia Cívica Municipal.

4.1 Alto volumen
4.2 Infractores por falta administrativa
4.3 Mediación
4.4 Queja

5. Dirección de Ordenamiento Patrimonial.

5.1 Anuencias municipales para la venta y consumo de bebidas alcohólicas
5.2 Permiso de boteo
5.3 Cambio de titular del título a perpetuidad del panteón municipal
5.4 Instalación y operación de circos
5.5 Instalación y operación de juegos mecánicos
5.6 Permiso de anuncios
5.7 Permiso de espacios públicos
5.8 Permiso para ejercer el comercio ambulante en modalidad móvil
5.9 Permiso para ejercer el comercio ambulante en modalidad semifijo.
5.10 Ratificación de medidas
5.11 Reubicación de luminarias
5.12 Permiso de volanteo

SECRETARÍA DE FINANZAS Y TESORERÍA

6. Dirección de Ingresos

6.1 Sistema Predial
6.2 Modernización Catastral
6.3 Sistema Isai
6.4 Anuencias, exclusivos

6.5 Tarifa Especial

II.- Subsecretaría de Áreas Administrativas, integrada por:

7. Dirección de Adquisiciones

7.1. Tramite de inscripción/refrendo al padrón de proveedores y prestadores de servicios del municipio de San Nicolás de los Garza, Nuevo León.

8. Dirección de Recursos Humanos

8.1 Expedientes laborales del personal activo, baja y contrataciones.

SECRETARÍA DE SEGURIDAD PÚBLICA

9. Dirección de Grupos Especiales

9.1 Actas de entrevistas
9.2 Entrevista a Detenidos
9.3 Citatorios
9.4 Documento de lectura de derecho
9.5 Informe homologado
9.6 Inspección de personas y recorridos.
9.7 Puestas a disposición
9.8 Puesto de Control
9.9 Uso de fuerza
9.10 Entrega a menor o adulto mayor

10. Dirección de Prevención del Delito

10.1 Asesoría Jurídica
10.2 Consentimiento de acceso a albergue
10.3 Entrega familiar
10.4 Entrevista a inicial es CAIPA
10.5 Entrevista a victimas
10.6 Negativa de intervención
10.7 Negativa de traslado
10.8 Permanencia en la institución.

11. Dirección de Policía

11.1 Actas de entrevista
11.2 Dictamen Medico
11.3 Documento de lectura de derecho
11.4 Inspección de personas y recorridos
11.5 Informe policial IPH
11.6 Minuta

11.7 Puestas a disposición
11.8 Registro de control de seguridad de visitas a secretaria
11.9 Registro de control de visitas a detenidos.
11.10 Uso de fuerza
11.11 Entrega a Menor o Adulto Mayor.

12 .Dirección de la Academia.
12.1 Control de Acceso al Edificio a la Academia de Policía.

SECRETARÍA DE SERVICIOS PÚBLICOS
13. Dirección de Mantenimiento
13.1 Recepción, asignación, ejecución, notificación, captura de solicitudes y evaluación de solicitudes de servicio que brinda la Secretaria de Servicios Públicos.

SECRETARÍA DE OBRAS PÚBLICAS Y DESARROLLO URBANO
14. Dirección de desarrollo urbano
14.1 Recepción de trámites y solicitudes de ciudadanos.

15. Dirección de proyectos y supervisión
15.1 Recepción de trámites y solicitudes de ciudadanos.

SECRETARIA DE DESARROLLO HUMANO
16. Dirección de Educación
16.1 Recepción de oficios, listados y solicitudes de planteles educativos

17. Dirección de juventud
17.1 Actividades de recreación y esparcimiento.

18. Dirección de Bienestar Animal
18.1 Registro de servicios.

19 Dirección de Ciudad Positiva
19.1 Recepción de solicitudes para programas.

20. Dirección de Gestión Ciudadana.

20.1. Recepción de solicitudes

21. Dirección de atención ciudadana.
21.1 Listas de asistencia

22. Dirección de Fortalecimiento Comunitario.
22.1 Listado de ciudadanos

SECRETARÍA DE PARTICIPACIÓN CIUDADANA
23. Dirección de PAC
23.1 Instalación de contenedores
23.2 Instalación de reductores de velocidad
23.3 Retiro de reductores de velocidad
23.4 Reubicación de reductores de velocidad
23.5 Cambio de boyas por bordo / bordo por boyas
23.6 Registro y actualización de comités ciudadanos
23.7 Lista de asistencia
23.8 Integración del comité ciudadano (del acta circunstanciada)

24. Dirección de Comités de Seguridad
24.1 Alta a Comité
24.2 Chat de WhatsApp
24.3 Alta de prestadores de servicio

25. Dirección de Delegados Municipales
25.1 Lista de Asistencia
25.2 Alta Delegados
25.3 Consulta de Vecinos para Alta Delegados
25.4 Alta de Enlaces
25.5 Baja de Delegado
25.6 Papelería para Alta de Delegado

SECRETARÍA DE MOVILIDAD
26. Coordinación Administrativa
26.1 Tramite de citas para pláticas con grupos de alcohólicos anónimos por retención y liberación de licencias de conducir.
26.2 Contestación de recursos de inconformidad.
26.3 Liberación de Vehículos, Retención de Licencias y Permisos Viales.

27. Dirección de Infraestructura Vial
27.1 Tramite de permisos de exclusivos y tramite de cierre de calles
27.2 Siniestros con daños a la infraestructura municipal.

SECRETARÍA TÉCNICA
28 Dirección de Comunicación Social
28.1 Autorización de Reproducción de Imagen

29. Dirección de Gobierno Digital
29.1 Autorizaciones.

30. Unidad de Protección Ambiental y Cambio Climático.
30.1 Anual - Drive Thru
30.2 Control de reportes UPACC

31. Dirección de Mejora Regulatoria
31.1 Trámite protesta ciudadana

32. CENTRO INTEGRAL DE TRANSPARENCIA Y PROTECCIÓN DE DATOS PERSONALES.
32.1 Recepción de solicitudes de acceso a la información.

DIRECCIÓN GENERAL DE SALUD
33. Dirección de Servicios Médicos
33.1 Entrega de resultados médicos a archivo
33.2 Interpretación de Estudio.
33.3 Interpretación de ultrasonido obstétrico.
33.4 Registro de entrada y salida de expedientes clínicos.
33.5 Registro diario de pacientes atendidos en radiodiagnóstico.
33.6 Alta Voluntaria Testigos
33.7 Alta Voluntaria
33.8 Consentimiento informado para internamiento/vigilancia medica
33.9 Consulta externa particular (Historia Clínica)
33.10 Exámenes médicos
33.11 Formato de defunción
33.12 Formato incapacidad por COVID-19
33.13 Nota de referencia y traslado
33.14 Nota Médica
33.15 Oficio de atención externa
33.16 Receta médica para población abierta
33.17 Receta médica
33.18 Registro diario de consulta externa
33.19 Censo Nominal para registro de vacunación
33.20 Entrega de pacientes
33.21 Hoja de pertenencia
33.22 Hoja diaria de enfermería triage (particular)
33.23 Hoja diaria de enfermería triage (derechohabientes)
33.24 Registro de Antígeno Prostático Específico

33.25 Registro de aplicación de flúor.
33.26 Registro de aplicación de vacuna COVID
33.27 Registro de capacitación en autoexploración de mama.
33.28 Registro de control de embarazo.
33.29 Registro de detección oportuna de cáncer
33.30 Registro de Entrega de Albendazol.
33.31 Registro de entrega de vida suero oral.
33.32 Registro de glucemias capilares.
33.33 Registro de métodos de planificación familiar
33.34 Registro de signos vitales
33.35 Registro de toma de Presión arterial.
33.36 Registro para aplicación de vacuna de influenza
33.37 Resultados de pruebas COVID 19
33.38 Carta de Buena Salud
33.39 Carta de Manejadores de alimentos.
33.40 Evaluación Médica de Aspirantes.

34. Dirección de Municipio Saludable

34.1 Acta Constitutiva.
34.2 Brigadas médicas en escuelas.
34.3 Dictámenes Médicos.
34.4 Formato de conformidad
34.5 Formato de orden y acta de verificación sanitaria.
34.6 Lista de asistencia del Comité Municipal.
34.7 Lista de asistencia para cursos, talleres y /o feria de salud.
34.8 Manejadores de alimentos ambulantes.
34.9 Registro de pacientes y servicios otorgados.
34.10 Servicio de fumigación.
34.11 Servicios otorgados.
34.12 Visitas médicos asistenciales.

CONTRALORÍA MUNICIPAL

35. Dirección de Auditoría

35.1 Recepción de quejas/denuncias ciudadanas.

36. Órgano Interno de Control

36.1 Base de datos de la recepción de quejas interpuestas en contra de elementos de la Secretaria de Movilidad.

37. Dirección de Asuntos Internos.

37.1 Base de datos o sistema de tratamiento. Base de datos de la recepción de quejas interpuestas en contra de elementos de la Secretaria de Seguridad Pública.

DIRECCIÓN GENERAL DE BIENESTAR SOCIAL

38. Dirección de Asistencia Humana y Comunitaria

38.1 Entrega de apoyos asistenciales
38.2 Actividades en Centros Comunitarios
38.3 Listas de Asistencia de clases

39. Dirección de Promoción Humana

39.1 Alta de maestras
39.2 Lista de asistencia a juntas del voluntariado de ANSPAC.
39.3 Listas de Asistencia de clases
39.4 Formato de entrega de manualidades
39.5 Lista de asistencia a certificaciones
39.6 Lista de asistencia a eventos
39.7 Préstamo de llaves de acceso a los módulos

40. Dirección de Grupos Vulnerables

40.1 Lista de asistencia "CASA CLUB DEL ADULTO MAYOR"
40.2 Lista de asistencia y servicios otorgados "ATENCIÓN PSICOLÓGICA
40.3 Lista de asistencia "CENTRO DE AUTISMO"
40.4 Solicitud de ingreso a ESTANCIAS INFANTILES
40.5 Bitácora de Servicios, TERAPIAS DE REHABILITACIÓN"

41. Dirección de la Mujer

41.1 Curso de Corte y Confección
41.2. Curso de Repostería
41.3 Curso Esmaltado en Gelish
41.4 Curso Diseño Social
41.5 Curso de Fotografía
41.6 Mujer Creativa
41.6 Grupo de Emprendedoras
41.7 Expo Mujer
41.8 Cine Debate
41.9 Círculos de Lectura
41.10 Red de Mujeres
41.11 Mujer una Vida Libre de Violencia
41.13 El Poder de ser Niña
41.14 Servicios para Atender a la Mujer
41.15 Servicios a Través de Puerta Violeta

42. UNIDAD GERONTOLOGICA
42.1Expediente Clínico.
42.2 Inscripción y Asistencia.

COORDINACION ESTRATEGICA DE GABINETE

43. Dirección de Consulta y Evaluación y de Reconstrucción del Tejido Social (RTS)
43.1 Listas de Asistencia, Evidencias Fotográficas, Videos Testimonio

A continuación, se señalarán cada uno de los Sistemas de tratamiento o bases de datos, indicando cuál es su estructura, así como las funciones y obligaciones de los servidores que realicen el tratamiento de datos personales en sus actividades.

Hipervínculo donde podrá ser visualizado:

https://drive.google.com/file/d/1YIdGJlSmQCBd0T8VPnZNnsnPal-Dan6I/view?usp=sharing

MEDIDAS DE SEGURIDAD FISICAS Y ADMINISTRATIVAS IMPLEMENTADAS EN MUNICIPIO DE SAN NICOLAS DE LOS GARZA

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

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.
I. 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.
II. 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.
III. Implementar programas de capacitación en materia de protección de datos personales al interior del Municipio.

Medidas de seguridad en el entorno

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

I. Registrar a visitantes que accedan a instalaciones;

II. Identificar a los servidores públicos adscritos al sujeto obligado, los cuales deberán portar la identificación deberá ser expedida y firmada por autoridad competente, e incluir cuando menos, nombre, cargo y número de empleado, fotografía, nombre de la Dependencia de su adscripción y unidad administrativa a la que pertenece. gafete de identificación dentro de las instalaciones.

Medidas de seguridad técnicas

Las medidas de seguridad técnicas consisten en mecanismos que se valen de la tecnología, aseguran el acceso a las bases de datos relacionados con el software y hardware, es decir protegen el entorno digital de los datos personales.

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

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 Dirección de Informática y Gobierno Abierto para efectos del soporte informático requerido;

III. Verificar que durante los mantenimientos y monitoreo que el personal interno 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.

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, en coordinación con la Dirección de Gobierno Digital y Dirección de Informática y Gobierno Abierto, implementarán cuando menos las siguientes medidas de seguridad en equipos computacionales que contengan documentos, archivos o sistemas de datos personales:

I.- Limitar o restringir por completo el uso de internet en los equipos que se estime pertinentes.

Medidas de seguridad para prevenir accesos no autorizados en las instalaciones.

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

Medidas de seguridad en caso de desastres naturales.

Tormentas eléctricas: En caso de que haya una interrupción de la energía eléctrica, cada equipo de cómputo cuenta con un regulador de corriente que ayuda evitar que ocasione daños en aparatos electrónicos de las Unidades Administrativas.

Inundaciones y Humedad: Los equipos de cómputo se encuentran situados sobre los escritorios para el caso de inundaciones.

Medidas de seguridad para acceder a los archiveros y gavetas.

Otra forma de evitar el acceso no autorizado, es limitar el fácil acceso a los sitios en los que se almacena la información; el Municipio de San Nicolás de los Garza se conforma por áreas administrativas, cada área cuenta con un sitio de resguardo en este apartado hablaremos de los sitios físicos los cuales son, archiveros y gavetas, mismos que se encuentran ubicados en los lugares de trabajo de cada servidor público adscrito a las diferentes áreas administrativas que conforman este sujeto obligado, las medidas de seguridad para un adecuado resguardo de los documentos que contienen datos personales son los siguientes:

Archiveros Físicos: Cada archivero cuenta un cerrojo para prevenir el acceso no autorizado a los documentos que se encuentran en su interior.

Gavetas: Por otra parte, existen gavetas que forman parte de los escritorios de los servidores públicos adscritos a las diferentes áreas administrativas, mismas que cuentan con llave.

Vigilancia en las instalaciones del Municipio de San Nicolás de los Garza.

Muchas de las medidas tomadas para garantizar la seguridad para prevenir injerencias humanas, ya sea deliberadas o accidentales, es colocar componentes clave como cámaras de seguridad, los cuales se describen a continuación.

Cámara de seguridad: Las cámaras que utiliza este sujeto obligado se encuentran posicionadas en puntos estratégicos para video grabar en los lugares con más tráfico de personas.

TECNICAS

Por otro lado, las medidas de seguridad técnicas, según la definición señalada en la legislación general de la materia, 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 los recursos involucrados en su tratamiento.

En ese sentido, y debido a que este órgano autónomo cuenta con equipo compuesto por hardware y software, se ilustran enseguida las diversas medidas técnicas con las que se cuenta.

1.-Medidas de seguridad para prevenir accesos no autorizados a equipos de cómputo.

A fin de evitar los accesos no autorizados a equipos de cómputo, se ha implementado el uso de usuarios y contraseñas para los empleados, mismas que son asignadas a los servidores públicos al ingresar a laborar, por lo que a través de las mismas se otorga un acceso limitado al ordenador.

2.-Medidas para prevenir virus informáticos y amenazas externas en la red.

Cada computadora de este organismo se encuentra protegida con un antivirus cuya función es detectar y eliminar virus informáticos que puedan dañar las bases de datos contenidas en los equipos de cómputo.

Asimismo, para garantizar la seguridad de la información, se cuenta con tres capas de seguridad, la primera por medio de hardware que involucra firewall y equipos de comunicación, la segunda capa por medio de software de seguridad para prevenir el hackeo o malware, spam o virus, la tercera capa por medio de sistemas operativos robustos con cifrados de seguridad en la transportación de los datos y mecanismos de auto respaldo.

4.-¿Por quién puede ser instalado el antivirus?
Cada equipo cuenta con una clave y contraseña la cual solo es de conocimiento de los servidores públicos adscritos al área de Informática y Sistemas, ellos se encargan de instalar el antivirus y darles mantenimiento a las máquinas de cómputo.

5.- Copias de seguridad o respaldos de la información.
Como medida de seguridad contra pérdida o destrucción de documentos electrónicos, se realiza una copia o respaldo de los documentos que se encuentren resguardados en los equipos de cómputo en una carpeta compartida.

6. Formas de supresión y borrado seguro de información, cuyo contenido se encuentran inmersos datos personales.

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.

ANALISIS DE RIESGOS

El análisis de riesgo tiene como objetivo alinear la protección de los datos personales que se traten en el Municipio de San Nicolás de los Garza, 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 San Nicolás de los Garza, 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	Afecta al ejercicio de derechos fundamentales y libertades públicas establecidos en la Constitución, y sus consecuencias son irreversibles. Las consecuencias están relacionadas con categorías especiales de datos o relativos a infracciones penales, y es irreversible. Causa un daño social significativo, como la discriminación, y es irreversible. Afecta a interesados en situación de especial vulnerabilidad, en particular niños, y de forma irreversible. Causa pérdidas morales o materiales Significativas e irreversibles.
Significativo	Los casos anteriores cuando los efectos son reversibles. Pérdida de control del interesado sobre sus datos personales, cuando la extensión de los datos sea alta con relación a las categorías de la extensión de los datos sea alta con relación a las categorías de datos o número de sujetos. Se produce o puede producirse usurpación de la identidad de los interesados. Pueden producirse pérdidas financieras significativas a los interesados y/o pérdida de confidencialidad de datos sujetos al deber de secreto profesional o vulneración del deber de confidencialidad.

	Existe un perjuicio social para los interesados o determinados colectivos de interesados.
Limitado	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. Pérdidas financieras insignificantes e irreversibles y/o Perdida de confidencialidad de datos sujetos al secreto profesional pero que no sean categorías especiales o sobre infracción penales 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. Pérdidas financieras insignificantes e irreversibles y/o Perdida de confidencialidad de datos sujetos al secreto profesional pero que no sean categorías especiales o sobre infracción penales
Muy Limitado	En el caso anterior, cuando todos los efectos son reversibles.

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

Riesgo de 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. 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.

Alto	Cuando se materializó el riesgo en el último año en alguna entidad. Existen estudios que determinan que la probabilidad podría ser alta. Existen auditorias o estudios que identifican posibles vulnerabilidades en los procedimientos organizativos o medios técnicos vinculados con dicho riesgo. Los elementos vinculados con los factores de riesgo se han implementado con tecnologías o procedimientos organizativos no maduros, sin seguir normas de calidad, sin estar certificados por terceros independientes.
Baja	Antecedente de una materialización de dicho riesgo en los últimos 10 años en alguna entidad
Improbable	Cuando no existe evidencia de la materialización de dicho riesgo en ningún caso.

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

Tipo de dato o información	Nivel de riesgo
Documentos personales: • Correos electrónicos • Actas de nacimiento • Curp • Identificaciones • Documentos Académicos • Documentos patrimoniales • Entre otros.	Medio

Aspectos personales: • Personas o grupos con los que se relaciona • Temperamento • Carácter • Inteligencia • Roles sociales • Capacidad de adaptación • Tolerancia de riesgo • Gustos / preferencias de contenidos audiovisuales (televisión interactiva, plataformas de contenidos, redes sociales,..) • Cuidado de salud • Culturales(lectura, música, arte,..) • Pertenencia y actividades en asociaciones sociales y culturales • Entre otros.	Alto
Preferencias de consumo, hábitos, gustos; necesidades, etc. que no permitan inferir informaciones relacionadas con categorías especiales de datos: • Preferencias de consumo categoría de comercio, tipo de establecimiento; tipo de productos; etc. • Hábitos de consumo • Preferencias de contenidos audiovisuales en diferentes medios (televisión interactiva, plataformas de contenidos, redes sociales, ..) • Preferencias de ocio (deportes, restaurantes, museos, teatros, música, etc.) • Entre otros	Bajo
Rendimiento laboral: • Control de acceso al lugar de trabajo • Grabación de imágenes en zonas de acceso o en oficinas • Grabación de audio en zonas de acceso o en oficinas. • Monitorización de los equipos de los empleados • Inferencia del rendimiento a través de indicadores (Productividad y calidad del trabajo, Eficiencia, Formación adquirida, objetivos conseguidos) • Entre otros	Medio
Situación económica: • Renta personal • Ingresos mensuales • Patrimonio (bienes muebles/inmuebles) • Entre otros.	Medio

Estado financiero: • Solvencia financiera • Pasivos (gastos en alimentación, vivienda, educación, salud, impuestos, pagos de créditos, tarjetas de crédito o gastos personales, etc.; • Nivel de deuda (Préstamos personales, hipotecas) • Ingresos. • Entre otros.	Muy Alto
Información Bancaria: • Cuentas bancarias. • Tarjetas. • Entre otros.	Muy Alto
Datos de comportamiento de empleados: • Fiabilidad de la persona • Hábitos y valores que facilitan la convivencia • Hábitos y valores' que facilitan el trabajo y el estudio • Hábitos y valores que influyen en el bienestar personal, laboral y familiar • Hábitos y valores que influyen en el compromiso con las personas y con la sociedad • Estabilidad laboral. • Antecedentes de comportamiento. • Entre otra información.	Medio
Datos de localización: • Registro de desplazamientos • Registro de lugares habituales • Registro de rutinas en base a localización • Registro de lugares habituales	Medio
Datos de Salud: • Historia clínica • Informes de salud • Informes de baja laboral por motivos de salud para el Servicio de Prevención de Riesgos Laborales • Recetas médicas • Datos relativos a salud física • Datos relativos a salud mental • Datos relativos a prestación de servicios de atención sanitaria • Documentos relativos a procesos asistenciales del paciente (incluida identificación de médicos y demás profesionales que han intervenido) • Cualquier información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. • Datos Genéticos	Alto

Datos biométricos: • Huella dactilar • Facciones rostro • Iris • Venas de la palma de la mano • Voz • Oreja • Gestos • Modo de andar • Descriptores corporales de cualquier índole • Trazos (firma)	Alto
Datos personales relativos a probables delitos e infracciones administrativas.	Muy Alto
Metadatos: • Datos de tráfico de las comunicaciones electrónicas • Identificación de emisor y/o receptor en las comunicaciones • Datos en conexiones a internet: localización; características software y hardware del dispositivo con el que se conecta; redes sociales o páginas en general en las que se ha logado, conexión (IP, proveedor de servicios, velocidad de descarga). • Entre otros.	Medio
Datos de Identificación: • Nombre • Estado Civil • Fecha de Nacimiento • Nacionalidad • Lugar de nacimiento • Domicilio • Teléfono • Correo electrónico • Firma autógrafa • Firma electrónica • Edad imagen	Bajo

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

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 San Nicolás de los Garza, se establecerá la probabilidad de que se materialice el impacto de vulnerabilidad con la cantidad de titulares que se establecen en los tratamientos; lo anterior de 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 San Nicolás de los Garza 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	Numero de Titulares	Nivel de Riesgo
ACTIVIDAD				
Perfilación: • Creación de perfiles • Uso de perfiles • Clasificación de individuos • Orientación de productos/servicios a individuos o grupos • Análisis comportamental (evaluación y calificación de emociones, estados de ánimo, hábitos, preferencias, etc.) Entre otros que pudieran derivar.	Alto	Acceso no autorizado al rastro digital de las y los usuarios, vulnerando la información de acuerdo al comportamiento de que se trate o finalidad de la actividad.	+ 5,000	3
Predicción: • Inferencia de nuevos datos personales. • Modificaciones. • Entre otros que pudieran derivar	Alto	Vulneración de registros de todos los datos personales de servidores públicos y usuarios que han otorgado su consentimiento para automatizar sus datos	- 500	1

Control de los Servidores Públicos: • Evaluación del empleado • Observación del puesto de trabajo • Monitorización del puesto de trabajo • Grabación de imágenes en ámbito laboral • Grabación de audio en ámbito laboral • Monitorización por medio de imágenes en ámbito laboral • Monitorización por medio de sonido en ámbito laboral • Tiempo invertido en realizar tareas • Monitorización y control de correo electrónico • Control de Asistencia. • Control de uso de teléfono Entre otros que pudieran derivar.	Medio	Información de lugar, tiempo y hora donde radican los servidores públicos, así como los cambios de turno, modo y lugares de vigilancia.	+ 50,000	3
Control del Acceso a Internet: • Análisis o evaluación de tiempos de uso de Internet • Control de permisos para actividades de navegación en Internet • Análisis o evaluación de alarmas sobre navegación a sitios específicos en Internet • Análisis o evaluación de alarmas sobre navegación a contenidos específicos en Internet Entre otros que pudieran derivar.	Medio	Vulneraciones a las 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
Observación: • Vigilancia mediante imágenes • Vigilancia mediante sonidos Vigilancia de comunicaciones • Vigilancia de Internet Entre otros que pudieran derivar.	Alto	Vulneración a la video vigilancia de los edificios y centros físicos del Municipio, así como de las comunicaciones oficiales e información en la nube	+50,000	3

Monitorización: •Control mediante imágenes Control mediante sonidos • Control de comunicaciones • Control de transmisiones • Control de internet Entre otros que pudieran derivar	Alto	Vulneración a los centros de control físicos y virtuales, así como a las redes comunicaciones de datos y la ubicación de los mismos.	+50,000	3
Supervisión: • Control • Análisis mediante imágenes • Análisis mediante sonidos • Análisis de comunicaciones • Análisis de transmisiones • Análisis de Internet • Control de tráfico rodado Entre otros que pudieran derivar.	Alto	Acceso no autorizado a la información relativa a la supervisión de actividades de las y los servidores públicos.	+50,000	3
Control físico de acceso: • Control de acceso a las instalaciones • Control de acceso a eventos • Control de acceso a instalaciones deportivas •Control de acceso a las áreas en específico. Entre otros que pudieran derivar.	Bajo	Acceso de personas no autorizadas a la inforamcion de quienes accedan a las instalaciones o quienes acuden a los eventos del Municipio, vulnerando su informacion que les es recabada.	+50,000	1
Decisiones automatizadas sin intervención humana.	Alto	No aplica		

Decidir sobre o impedir el ejercicio de derechos fundamentales: • Derecho a la igualdad • Derecho a la no discriminación • Derecho a la vida y a la integridad física • Derecho a la libertad religiosa • Derecho a la libertad personal • Derecho al patrimonio • Derecho a la intimidad personal y familiar • Derecho a la propia imagen • Derecho a la libertad de expresión e información • Derecho a la libertad de cátedra • Derecho a la libertad de reunión • Derecho a la libertad de asociación • Derecho al libre acceso a cargos y funciones públicas en condiciones de igualdad • Derecho a la legalidad penal • Derecho a la educación • Derecho a la libertad sindical • Derecho de peticiónOtros derechos consagradas en Política de los libertades la Constitución Estados Unidos Mexicanos.	Alto	Vulneración a los procesos que se llevan a cabo en el Municipio, referentes a solicitudes, servicios, procedimientos, dudas o quejas, asi como cualquiera que se encuentre dentro de las facultades del Municipio de San Nicolas de los Garza.	+500,000	3
Decidir sobre el control del interesado de sus datos personales: • Derecho de acceso • Derecho de rectificación • Derecho de oposición • Derecho de Cancelación • Derecho a la portabilidad	Alto	Privar de los derechos de los titulares en materia de protección de datos personales	+500,000	3
Decidir sobre el acceso a un servicio de los que presta el Municipio de San Nicolás de los Garza	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 informacion	+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 trámites que tengan efectos jurídicos sobre las personas	Alto	Anticipacion a las resoluciones y manipulacion o sustraccion de personas y/o tramites.	+50,000	3
Servicios de Salud.	Alto	Vulneracion a la intimidad de las personas y riesgo de discriminación.	+5,000	2
Conservacion con fines de archivo	Medio	Vulneracion a toda la informacion o perdida de la misma en archivos fisicos como electronicos.	+500,000	3
DATOS PERSONALES				
Documentos Personales •Correos electrónicos • Actas de Nacimiento •Curp •identificaciones •Documentos académicos •Documentos patrimoniales Entre otros.	Medio	Vulneracion a la informacion personal de identificacion, academica y patrimonial de usuarios y servidores publicos.	+500,000	3
Aspectos personales: • Personas o grupos con los que se relaciona • Temperamento • Carácter • Inteligencia • Roles sociales • Capacidad de adaptación • Tolerancia al riesgo • Gustos/preferencias de contenidos audiovisuales (televisión interactiva, plataformas de contenidos, redes sociales, ...) • Cuidado de salud •Culturales (lectura, música, arte, ...) Pertenencia actividades en asociaciones sociales y culturales Entre otros	Alto	Vulneracion de datos que identifican a las personas de acuerdo a sus aspectos personales, pudiendo catalogar a las personas de acuerdo a sus interesres personales	+50,000	3

Preferencias de consumo, hábitos, gustos, necesidades, etc. que no permitan inferir informaciones relacionadas con categorías especiales de datos: • Preferencias de consumo: categoría de comercio, tipo de establecimiento; tipo de productos; etc. • Hábitos de consumo • Preferencias de contenidos audiovisuales en diferentes medios (televisión interactiva, plataformas de contenidos, redes sociales. • Preferencias de ocio [deportes, restaurantes, museos, teatros, música, etc.)Entre otros	Bajo	Vulneración de 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
Rendimiento laboral: • Control de acceso al lugar de trabajo • Grabación de imágenes en zonas de acceso o en oficinas • Grabación de audio en zonas de acceso o en oficinas. • Monitorización de los equipos de los empleados • Inferencia del rendimiento a través de indicadores (Productividad y calidad del trabajo, Eficiencia, Formación adquirida, objetivos conseguidos) Entre otros	Medio	Vulneración al modo de trabajo de las personas, así como a la privacidad en sus centros de trabajo.	+5,000	2
Situación económica: • Renta personal • Ingresos mensuales • Patrimonio (bienes muebles/inmuebles) • Situación laboral Entre otros.	Medio	Puede ocasionar discriminación o bien ser objetivos para fraudes o extorsiones.	+50,000	3

Estado financiero: • Solvencia financiera • Pasivos (gastos en alimentación, vivienda, educación, impuestos, pagos de tarjetas de crédito o salud, créditos, gastos personales, etc.; • Nivel de deuda (Préstamos personales, hipotecas) • Ingresos. Entre otros.	Muy Alto	Puede ocasionar discriminación o bien ser objetivos para fraudes o extorsiones.	+5,000	5
Información Bancaria: • Cuentas bancarias. • Tarjetas. Entre otros.	Muy Alto	Puede ocasionar discriminación o bien ser objetivos para fraudes o extorsiones.	+5,000	5
Datos de comportamiento de empleados: •Fiabilidad de la persona • Hábitos y valores que facilitan la convivencia •Hábitos y valores que facilitan el trabajo y el estudio • Hábitos y valores que influyen en el bienestar personal, laboral y familiar • Hábitos y valores que influyen en el compromiso con las personas y con la sociedad • Estabilidad laboral. • Antecedentes de comportamiento. Entre otra información.	Medio	Pueden ser objetos de algún tipo de distinción o de ataques sociales por su comportamiento laboral y académico.	+5,000	2
Datos de localización: • Registro de desplazamientos • Registro de lugares habituales • Registro de rutinas en base a localización Registro de lugares habituales	Medio	Puede ser objeto de ataques, fraudes o extorciones el conocer donde se desplazan las y los servidores publicos, los lugares a los que acuden con frecuencia asi como sus rutinas y horarios.	-500	1

Datos de Salud • Historia clínica • Informes de salud • Informes de baja laboral por motivos de salud para el Servicio de Prevención de Riesgos Laborales • Recetas médicas • Datos relativos a salud física •Datos relativos a salud mental •Datos de la prestación de servicios de atención sanitaria •Documentos relativos a procesos asistenciales del paciente (incluida identificación de médicos y demás profesionales que han intervenido • Cualquier información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. • Datos Genéticos	Alto	Pueden ser objeto de ataques a la privacidad personal, discriminación, manipulación, o perjuicio moral.	+5,000	3
Datos biométricos: • Huella dactilar • Facciones rostro, Iris • Venas de la palma de la mano • Voz, Oreja, Gestos • Modo de andar •Descriptores corporales de cualquier índole •Trazos (firma)	Alto	Vulnera los datos de autentificación, lo cual puede traer para las personas perjuicio económico, patrimonial y laboral.	+5,000	3
Categorías especiales de datos o que permitan inferirlos: • Origen étnico • Origen racial • Opiniones políticas •Convicciones religiosas • Convicciones filosóficas • Afiliación sindical • Datos relativos a la salud • Datos de la vida sexual • Datos relativos a las orientaciones sexuales Entre otros.	Alto	La vulneración de esta información personal tendría consecuencias morales y sociales ya que pueden ser objeto de discriminación si se difunde esta información o si se tienen accesos no autorizados.	+5,000	3

Datos personales probables delitos relativos a e infracciones administrativas.	Muy Alto	Puede traer consecuencias de daño moral y físico contra la persona que se encuentre ante proceso de esta índole.	+500,000	5
Metadatos: • Datos de tráfico de las comunicaciones electrónicas • Identificación de emisor y/o receptor en las comunicaciones •Datos en conexiones a internet: localización; características software y hardware del dispositivo con el que se conecta; redes sociales o páginas en general en las que se ha logado, conexión (IP, proveedor de servicios, velocidad de descarga). Entre otros.	Medio	Identificación del movimiento, comunicación y actualización de la información, así como de las conexiones de red, lo cual podría poner en riesgo los sistemas internos así como los equipos de cómputo.	+5,000	3
Datos de Identificación: • Nombre • Estado Civil • Fecha de Nacimiento. • Nacionalidad • Lugar de nacimiento • Domicilio • Teléfono • Correo electrónico • Firma autógrafa • Firma electrónica • Edad imagen	Bajo	Acceso no autorizado a información del personal del Municipio, o bien a la información de las personas usuarias, vulnerándose su información personal de identificación y contacto.	+500,000	1
Categoría del Titular / Factor de riesgo				
Menores de 14 años	Muy Alto	Vulneración a información de menores de edad.	+50,000	5
Víctimas de violencia de genero	Muy Alto	Identidad de las victimas los 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 genero	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	+5,000	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

ANALISIS DE BRECHA

Para realizar el análisis de brecha, el Centro Integral de Transparencia y Protección de Datos Personales del municipio de San Nicolás de los Garza, elaboró un cuestionario; el objetivo del referido cuestionario es efectuar un auto diagnóstico que determine el nivel de desempeño real esperado en cuanto a las medidas de seguridad por parte de los empleados. Dicho cuestionario se aplicó a todo el personal del Municipio de San Nicolás de los Garza, derivado del estudio e identificados los posibles riesgos a los que el Municipio de San Nicolás de los Garza análisis de las respuestas allegadas en conjunto determinan el nivel de desempeño real por parte de los servidores públicos adscritos a las diferentes áreas administrativas de este sujeto obligado; a continuación se pone a su disposici6n el cuestionario en comento.

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?
Á.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 San Nicolás de los Garza, de acuerdo a las medidas que implementen dentro de sus labores cotidianas:

A.1. ¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?

SI = 92.8%

NO = 7.2 %

A.2. ¿Tienes mecanismos para eliminar de manera segura la información?

SI = 66.5.8%

NO = 33.5 %

A.3. ¿Has establecido y documentado los compromisos respecto a la protección de datos?

SI = 76.8%

NO = 23.2 %

A.4. ¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?

[redacted]

Á.5. ¿Realizas respaldos periódicos de los datos personales?

SI = 56.5%

NO = 43.5 %

B.1. ¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?

SI = 74.8%

NO = 25.2 %

B.2. ¿Tienes medidas de seguridad para evitar el robo?

[redacted]

B.3. ¿Cuidas los movimientos de información en entornos de trabajo físico?

SI = 84.9%

NO = 15.1 %

C.1. ¿Realizas actualizaciones al equipo de cómputo?

SI = 65.6%

NO = 34.4%

C.2. ¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?

SI = 88.3%

NO = 11.7%

C.3. ¿Tienes medidas de seguridad para navegar en entornos digitales?

[redacted]

C.4. ¿Cuidas el movimiento de información en entornos de trabajo digitales?

SI =84.5%

NO = 15.5%

PLAN DE TRABAJO

Se ha planteado aplicar las medidas y métodos necesarios para llevar a cabo la implementación total de las medidas de seguridad faltantes en un periodo de doce meses a partir de la aprobación del presente documento de seguridad.
Por lo que, todas aquellas medidas de seguridad física y técnicas que requieran la erogación de recursos como la compra de bienes muebles, se realizaran conforme el presupuesto lo permita, por otro lado, las medidas que no requieran de la erogación de recursos, deberán ser implementadas de acuerdo con los tiempos administrativos del Sujeto Obligado.

MECANISMOS DE MONITOREO Y REVISION DE LAS MEDIDAS DE SEGURIDAD

A fin de supervisar y garantizar el cumplimiento y mejora continua de las medidas de seguridad que se encuentran implementadas en cuanto a la cultura de los empleados, el entorno de trabajo físico, así como el entorno de trabajo digital, se han definido controles de monitoreo periódico, que permitan el seguimiento de esas medidas, el cual será realizado por el Centro Integral de Transparencia y Protección de Datos Personales, y del cual se realizara un informe anual en el mes de diciembre, mismo que se pondrá a disposición del Comité de transparencia durante los primeros veinte días del mes de enero del siguiente año.

PROGRAMA GENERAL DE CAPACITACION

Para contribuir al fortalecimiento de la cultura de Protección de Datos Personales, la Dirección de Capacitación y Desarrollo Profesional de este Municipio, deberá implementar un programa General de Capacitación, dirigido a los servidores públicos adscritos a este sujeto obligado, a fin de mantenerlos actualizados en cuanto al debido tratamiento y protección de los datos personales y sistemas de tratamiento a los cuales tienen acceso. La finalidad del programa general de capacitación, es brindar los conocimientos y herramientas necesarias al personal, a fin de mejorar la gestión de sus sistemas de tratamiento, lo cual tendrá como consecuencia un incremento y mejora, en los niveles de seguridad.

TEMPORALIDAD

Las fechas para la implementación de las capacitaciones serán una vez al año, mismas que serán establecidas en base a la carga de trabajo de cada una de las áreas administrativas, asimismo, es de mencionarse que por necesidades particulares de cada área o por el ingreso de nuevo personal, se podrá solicitara a las instancias correspondientes, capacitaciones extraordinarias. Para el caso que en el transcurso del año se presente alguna modificación a la ley de la materia, surja alguna actualización en el tema, o alguna de las unidades administrativas tenga la necesidad de que se le capacite, se solicitara la programación del curso respectivo.

Finalmente el personal adscrito al Centro Integral de Transparencia y Protección de Datos Personales del Municipio de San Nicolás de los Garza, estará en constante capacitación, a fin de mantenerse actualizados en base a los estándares más altos de la información en materia de protección de datos personales, esto mediante cursos y/o talleres presenciales o en línea.

ACTUALIZACION DEL DOCUMENTO DE SEGURIDAD DEL MUNICIPIO DE SAN NICOLAS DE LOS GARZA.

El presente documento de seguridad se actualizara cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Se modifiquen las medidas de seguridad, derivado de las revisiones a las políticas en materia de protección de datos personales del Municipio de San Nicolás de los Garza;

III. Como resultado de un proceso de mejora continua para mitigar el impacto de una vulneración, e
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
V. Cuando surjan documentos, formatos, recomendaciones por parte del INFONL para la mejora del presente documento de seguridad.

Dado en el Comité de Transparencia de la Administración Pública del Municipio de San Nicolás de los Garza, Nuevo León, a los 26-veintiseis días del mes de marzo de 2024 dos mi veinticuatro.

COMITÉ DE TRANSPARENCIA DE LA ADMINISTRACIÓN PÚBLICA DEL MUNICIPIO DE SAN NICOLAS DE LOS GARZA

Arq. Alicia Rosalinda Avendaño Lozano **Presidente del Comité**	
Lic. Alfonso Jarero Gracia **Secretario Técnico**	C.P. Serafín Treviño Salinas **Vocal**
Lic. Rosalinda Guerra Hinojosa **Vocal**	Lic. Horacio Damián García Balderas **Vocal.**