



## **DOCUMENTO DE SEGURIDAD**

**EN MATERIA DE TRATAMIENTO DE DATOS  
PERSONALES, EN POSESIÓN DEL MUNICIPIO DE  
MARÍN, N.L.**

**ABRIL 2024**



# CONTENIDO

<b>INTRODUCCION.....</b>	<b>2</b>
1. MARCO JURIDICO.....	3
2. PROCESO METODOLÓGICO.PARA EL PROCESO DE ELABORACION DEL DOCUMENTO DE SEGURIDAD.....	4
3. AMBITO DE APLICACIONES Y GENERALIDADES.....	6
4. INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES	8
5. SISTEMAS DE TRATAMIENTO O BASES DE DATOS PERSONALES.....	9
6. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.....	135
7. MEDIDAS DE SEGURIDAD.....	138
A) ANALISIS DE RIESGO.....	141
B) ANALISIS DE BRECHA.....	144
C) PLAN DE TRABAJO.....	145
8. PLAN DE CONTINGENCIA.....	146
9. MECANISMO DE MONITOREO.....	147
10. PROGRAMA GENERAL DE CAPACITACION.....	147
11. ACTUALIZACIONES.....	148

# INTRODUCCIÓN

Las reformas constitucionales realizadas en 2009 y 2014 a los artículos 16 y 6, respectivamente, propiciaron por un lado la emisión de la ley en la materia con el propósito de garantizar este derecho fundamental y por otro fijar las bases para la emisión de la Ley General respecto a la Información en posesión de entes públicos.

Por otra parte, el 26 de enero de 2017, se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados -LGDPPSO- misma que establece las bases, principios y procedimientos para garantizar dicho derecho, siendo aplicable en los tres niveles de gobierno; con lo que se definen las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

En relación al nivel estatal, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado del Nuevo León -LPDPPSO-, se publicó en el Periódico Oficial del Estado el 11 de diciembre de 2019; por lo que todos los entes públicos, al llevar a cabo el tratamiento de los datos personales de personas físicas, adquieren el carácter de Responsable y deberán tratar dichos datos conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, responsabilidad; adoptar medidas de seguridad en atención a los sistemas de datos que traten; consignar dichas medidas en un documento de seguridad, garantizar el ejercicio de los derechos ARCO, entre otras obligaciones.

Desde el inicio de la Presente Administración 2021-2024 del Gobierno Municipal de Marín, N.L. a través de la Unidad de Transparencia, y en conjunto con los enlaces que se tiene en cada área generadora de información, se han realizado acciones y actividades que tuvieron como finalidad establecer los cimientos para la creación de este documento, en el cual se describa y se dé cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que poseen de conformidad a lo previsto en el artículo 41 de la Ley estatal.

## **MARCO JURIDICO**

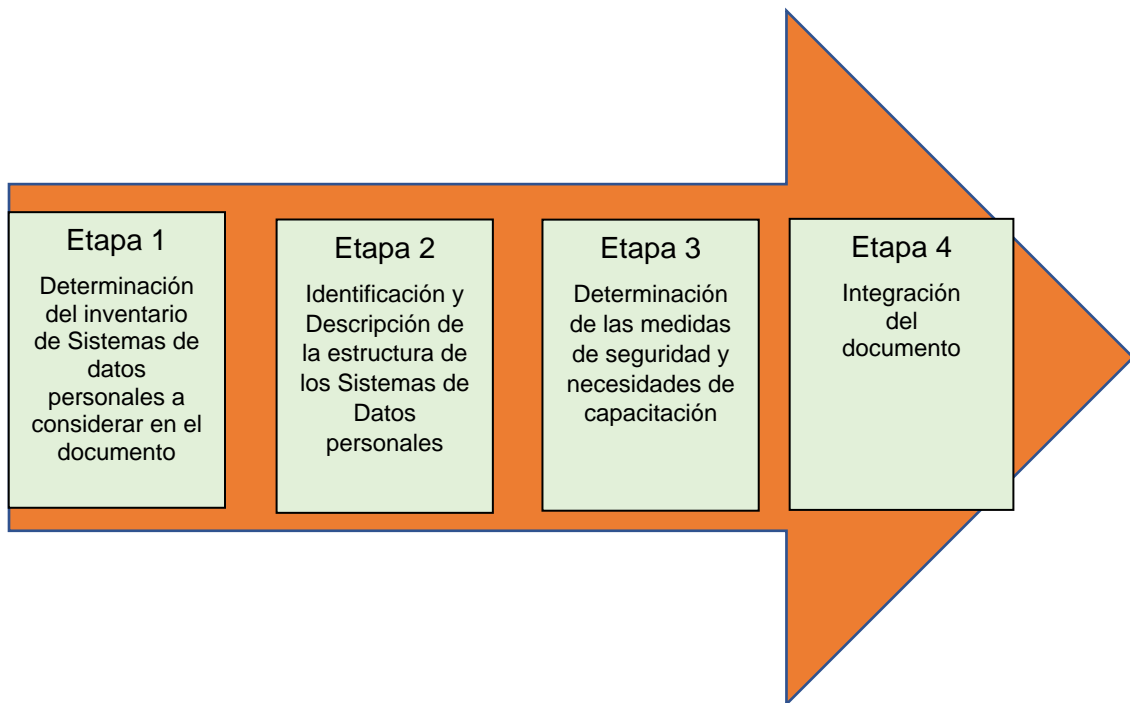
Para efectos del presente documento, la normatividad aplicable comprende la siguiente:

- Constitución Política de los Estados Unidos Mexicanos
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados publicada el 26 de enero de 2017 en el Diario Oficial de la Federación
- La Constitución Política del Estado Libre y Soberano de Nuevo León
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León
- Ley de Gobierno Municipal del Estado de Nuevo León
- Reglamento de la Administración Pública Municipal de Marín, N.L.
- Acuerdo 37/2023 del Instituto Estatal de Transparencia N.L. aprobando el Programa Anual de evaluación en materia de protección de datos personales para los sujetos obligados”

# PROCESO METODOLÓGICO PARA LA ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD

Para la elaboración del presente documento de seguridad y para dar cumplimiento a lo establecido en la Ley, se definió el siguiente desarrollo que comprendió las siguientes etapas:

## Proceso de Construcción



La coordinación en la elaboración del presente “DOCUMENTO DE SEGURIDAD” estuvo a cargo de la Unidad de Transparencia, llevándose a cabo lo siguiente:

- Se integraron los requisitos mínimos que debería contener de conformidad con la normatividad aplicable.
- Se realizaron reuniones con las secretarías y direcciones del Gobierno Municipal de Marín, N.L., con la finalidad de conocer el inventario de sistemas electrónicos y físicos en el municipio; así como para conocer medidas de seguridad que deben prevalecer en los sistemas soporte electrónico, desde el punto de vista de la infraestructura tecnológica y de comunicaciones, así como de las de seguridad de información que establece el manual de políticas correspondiente,
- Se solicitó información para la integración del inventario y se comunicó la metodología y un ejemplo, realizándose reuniones de trabajo virtuales para explicar y aclarar los formatos

y sobre la información requerida, y determinar la susceptibilidad a incorporarse en los formatos determinados.

- Las áreas que cuentan con sistemas o bases de datos personales, proporcionaron a la Unidad de Transparencia, la información correspondiente a su objetivo y su fundamento normativo. Así como, la Identificación y descripción de la estructura de los mismos, el tipo de datos y su idoneidad, la forma de obtención, el administrador de los sistemas, operadores, usuarios, tipo de soporte, características del lugar en que se localizan, su portabilidad, si existe transferencia y si en su caso hay encargados.
- Respecto a las medidas de seguridad se verifico la identificación de las existentes, y la determinación de brechas con base en el análisis de riesgos, estableciendo un plan de trabajo, mecanismos de monitoreo y un plan de contingencia.
- Se determinó un programa general de capacitación. Con dicha información se integró el presente documento de seguridad.

En esencia el documento de seguridad se integra por el inventario de los sistemas de tratamiento, las funciones y obligaciones de las personas que tratan datos personales, el análisis de riesgo y de brecha, el plan de trabajo, los mecanismos de monitoreo y revisión de las medidas de seguridad, plan de contingencia y el programa general de capacitación.

Para su plena vigencia el presente documento deberá ser aprobado por el Comité de Transparencia del Municipio de Marín, Nuevo León, quien es la máxima autoridad municipal en la materia.

## **AMBITO DE APLICACIÓN Y GENERALIDADES**

En cumplimiento a la LPDPPSO del Estado de Nuevo León, publicada el 11 de diciembre de 2019, el presente documento es aplicable a todas las dependencias y entidades municipales, que en ejercicio de sus atribuciones y funciones administran bases de datos en sistemas de tratamiento de datos personales, ya sean sistemas completos o el tramo de información que le corresponda.

También serán aplicables al tratamiento de datos personales que obren en soportes físicos y/o electrónicos, independientemente de su creación, procesamiento, almacenamiento y organización. Dichos datos podrán ser expresados en forma numérica, alfabética, gráfica. Alfanumérica, fotográfica, acústica o en cualquier otro formato.

Quienes tengan acceso a datos personales, están obligados a conocer y aplicar las medidas de seguridad del sistema en el que se concentren los datos y es aplicable en cada fase de su tratamiento, desde su obtención, hasta su eliminación. También se está obligado a su confidencialidad, aún después de su participación en el tratamiento, por cambio de funciones o por conclusión de la relación laboral. Así también, se tendrán las siguientes funciones y obligaciones en cualquier nivel de tratamiento:

### **Funciones genéricas**

El tratamiento de datos personales con responsabilidad, y las medidas de seguridad establecidas.

### **Obligaciones genéricas**

- Confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.
- Competencia en materia de tratamiento de Datos Personales.
- Informar al superior jerárquico, ante cualquier acción que pueda poner en riesgo los datos personales y en general que puedan vulnerar su seguridad.

De acuerdo a los cargos, encargos y/o designaciones se definen cuatro roles básicos en el tratamiento de los datos personales: Responsables del Sistema, Administrador del Sistema, Operadores y Enlace de datos personales (figura en proceso de asignación)

**Administrador Responsable del Sistema.** El titular de la dependencia o entidad que administre el sistema, quien deberá dar aviso a la Dirección de Transparencia de los sistemas que involucran tratamiento de datos personales en dicha dependencia o entidad.

Validar la información entregada por los titulares de los datos personales, sea la estrictamente necesaria para cumplir con los fines legales para los cuales se hubieran recabado.

**Usuario Responsable del Sistema.** El director de área o a quien se designe de manera expresa. Tendrá a su cargo la responsabilidad de la Administración del Sistema, siendo responsable de:

- Mantener actualizado el Sistema
- Determinar quiénes deben tener acceso a los datos personales en función del tratamiento que debe aplicarse a los mismos
- Autorizar los accesos, determinar los privilegios y limitantes y llevar registro de los mismos.
- Implementar las medidas de seguridad con la finalidad de evitar vulneraciones de la información.

**Encargado y/o Enlace de datos personales.** Será el Enlace de la Dirección de Transparencia, quien deberá de conocer el inventario de sistemas que involucren tratamiento de datos personales y por cada uno conocer el tipo de datos personales que se recaban y el nombre del encargado por cada Sistema.

Dar seguimiento a las acciones de capacitación al personal involucrado en el tratamiento de datos personales.

Atender requerimientos de información que solicite el Instituto de Transparencia del Estado de Nuevo León y su Normatividad.



# INVENTARIO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES (Resumen)

AYUNTAMIENTO MARÍN, NUEVO LEÓN SECRETARÍAS Y/O DIRECCIÓN		
ORGANISMOS CENTRALIZADOS	NO. DE SISTEMAS	NOMBRE DE SISTEMAS
PRESIDENTE MUNICIPAL	1	Atención a la Ciudadanía
SINDICATURA MUNICIPAL	11	Constancia de Abandono de Hogar Acuerdos y Convenios Constancia de Buena Conducta Constancia Autorización de Menor Constancia de Exhumación Constancia de Identidad Constancia de No Afectaciones a Vía Pública Constancia de Separación Constancia de Tutor Constancia de Residencia Constancia de Unión Libre
TESORERIA MUNICIPAL	6	Catálogo de Proveedores Transferencias Electrónicas Cheques Nominativos Licencias de Conducir Recibo de Egresos (Apoyos) Predial
ORGANO INTERNO DE CONTROL	1	Procedimiento de Responsabilidad Administrativa
UNIDAD DE TRANSPARENCIA	1	Solicitudes de acceso, rectificación, cancelación y oposición de datos personales (ARCO)
DIF MUNICIPAL	6	Comedor Mixto Traslados Boletos de Autobús Despensa Municipal Terapia de Lenguaje Terapia Física
SECRETARIA DEL AYUNTAMIENTO	4	Constancia de Ingresos Constancia de Recomendación Constancia Laboral Expediente del 3er. Sector Saladito
DIRECCION DE DESARROLLO SOCIAL	1	Uniformes y útiles escolares gratuitos
DIRECCION DE EDUCACIÓN Y CULTURA	3	Biblioteca Diversas Expresiones Culturales Módulos Digitales
DIRECCIÓN DE DEPORTES	3	Eliminatoria De Olimpiadas Registro Área De Pesas Gimnasia
DIRECCION DE OBRAS PUBLICAS Y DESARROLLO URBANO	3	Asignación de números oficiales. Licencias de subdivisión y fusión de predios. Licencia de uso de suelo, edificación y construcción.
DIRECCION DE SERVICIOS PÚBLICOS	3	Atención a la Ciudadanía Programa de Limpieza (Ramas y Escombro) Programa Entrega Botes de Basura
DIRECCIÓN DE SEGURIDAD PÚBLICA Y TRÁNSITO	1	Certificación para licencias de conducir
<b>TOTAL DE SISTEMAS</b>	<b>44</b>	

# SISTEMAS DE TRATAMIENTO O BASES DE DATOS PERSONALES

Después del inventario inicial de datos personales, de las capacitaciones, el cuestionario y diversas gestiones con los enlaces de Transparencia de todas las dependencias del Gobierno Municipal de Ayutla, Jalisco, se diseñaron los sistemas de tratamiento, que se realizarán por las Diversas Secretarías y Direcciones que a continuación de describen:

## PRESIDENTE MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR			
<b>I.- Nombre del sistema:</b>		ATENCIÓN A LA CIUDADANÍA	
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>			
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
Administrador Responsable			
<b>Nombre:</b>	José Santamaría Gutierrez	<b>Cargo:</b>	Presidente Municipal
Usuario Responsable 1			
<b>Nombre:</b>	Kenia Jasmin Tristan Contreras	<b>Cargo:</b>	ASISTENTE
Encargado			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b>			
<b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Tener un control de los expedientes de los reportes al Gobierno Municipal de Marín, N.L. conforme a las Solicitudes que realiza cada Ciudadano		
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.		
<b>Datos Personales que se encuentran en el sistema:</b>	ORDINARIOS (Identificativos)		
	Dato Personal	Idoneidad	
	Nombre	Para la identificación	
	Domicilio	Para la identificación	
	Teléfono	Para la notificación en su caso	
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>		
<b>Volumen de Formatos</b>	<b>2,450 Expedientes</b>		
<b>Cantidad Global de Datos Personales</b>	<b>7,350 Datos Personales Tratados</b>		
<b>Quien suministra</b>	El ciudadano del Municipio de Marín, N.L.		
<b>Cómo suministra</b>	Directamente / Indirectamente		

<b>Forma de obtención de datos</b>	Formato					
<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para llevar control			
	<b>Documentos Adjuntos con protección de datos personales</b>		En algunos casos ( solo se pide copia de su ine para proceden con el seguimiento de los apoyos y/p tramites, según sea el caso)			
	<b>Características del lugar donde se resguardan</b>		ARCHIVERO DE OFICINA DEL PRESIDENTE MPAL			
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b> <b>VII.- Resguardo de los Sistemas</b> <b>XII.- Medidas de seguridad aplicadas a las instalaciones</b> <b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	SI	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	La memoria USB solo pertenece Al área de la Oficina del Presidente Mpal, donde ninguna persona ajena la puede usar, ya que se encuentra resguardada bajo llave y está libre de virus.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta area y solo se transfiere si lo solicitan las máximas autoridades (Tesorería y auditoria del estado)					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	La computadora solo pertenece al área, y ninguna persona, tiene acceso, asi mismo está libre de virus.					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección y solo se transfiere si lo solicitan las máximas autoridades (alcalde, secretario del ayuntamiento, tesorería y auditoria del estado).					

<b>Acceso a las instalaciones</b>						
Seguridad perimetral exterior: <b>SI SE CUENTA</b>						
Seguridad perimetral interior: <b>SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						
Soporte de la bitácora:	Físico	SI	Electrónico	NO	Otro:	NO
Lugar de almacenamiento:	ARCHIVERO OFICINA PRESIDENTE MPAL			Tiempo	3 AÑOS	
Como se asegura la integridad:	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
Datos que se registran: fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
Soporte del registro:	Físico	SI	Electrónico	USB	Otro:	NO
Lugar de almacenamiento:	OFICINA PRESIDENTE MPAL			Tiempo	3 AÑOS	
Como se asegura la integridad:	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
Tipo de respaldo:	Completo	NO	Diferencial	NO	Incremental	SI
Medios para almacenar copias de seguridad	Se generará respaldo cada que se tenga información nueva relacionada con el tema en una memoria USB, ordenada de manera cronológica.					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia	Si	X	NO			
Se realizan pruebas de eficiencia	Si	X	NO			
Se cuenta con un sitio redundante	Si	X	NO			
Procedimiento	NO APLICA					
Equipo	NO APLICA					
Personal	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
Datos del sistema que será cancelado: NO APLICA						
Denominación:	NO APLICA					
Motivos:	NO APLICA					
Plazos y condiciones para el bloqueo del sistema:						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: NO APLICA						
Procedimiento para la supresión y periodo de conservación del sistema: Por formateo						
Mecanismos para la supresión del sistema: En lo digital se formatea el equipo, en lo físico, se tritura la documentación obsoleta						

## SINDICATURA MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR					
<b>I.- Nombre del sistema:</b>		CONSTANCIA DE ABANDONO DE HOGAR			
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>					
Administrador Responsable					
<b>Nombre:</b>	Rosalba Carolina González Caballero	<b>Cargo:</b>	SINDICO DEL AYUNTAMIENTO		
Encargado					
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA		
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>					
<b>Objetivo:</b>	Brindar un documento cuando se presenta la situación que una persona abandona el hogar donde habitaba con su pareja.				
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.				
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)				
	<b>Dato Personal</b>		<b>Idoneidad</b>		
	Nombre		Para la identificación		
	Domicilio		Para la identificación		
	Teléfono		Para la notificación en su caso		
	Nombre de Hijos		Para la identificación		
	Años de Matrimonio o vivir juntos		Para la identificación		
	Nombres de Testigos		Para la identificación		
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>5 Datos</b>				
<b>Volumen de Formatos</b>	<b>2 Expedientes</b>				
<b>Cantidad Global de Datos Personales</b>	<b>10 Datos Personales Tratados</b>				
<b>Quien suministra</b>	El ciudadano del Municipio de Marín, N.L.				
<b>Cómo suministra</b>	Directamente				
<b>Forma de obtención de datos</b>	Constancias,				
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>
	<b>Tipo de Soporte</b>	SI			
<b>Descripción</b>	Formato establecido para hacer la constancia				

<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	INE, COMPROBANTE DE DOMICILIO Y EL INE DE 2 TESTIGOS				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE OFICINA DEL SINDICO MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el ciudadano lo autoriza					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						

<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SINDICO DEL AYUNTAMIENO			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Increment al	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SINDICATURA MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR					
<b>I.- Nombre del sistema:</b>		ACUERDOS Y CONVENIOS			
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>					
Administrador Responsable					
<b>Nombre:</b>	Rosalba Carolina González Caballero	<b>Cargo:</b>	SINDICO DEL AYUNTAMIENTO		
Encargado					
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA		
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>					
<b>Objetivo:</b>	Brindar un documento que se elabora entre dos o más personas en el cual se llega a distintos pactos.				
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.				
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)				
	<b>Dato Personal</b>		<b>Idoneidad</b>		
	Nombre		Para la identificación		
	Domicilio		Para la identificación		
	Teléfono		Para la notificación en su caso		
	Datos que trate el acuerdo (Monetarias y Pertenencias)		Acuerdo Mutuo		
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>4 Datos</b>				
<b>Volumen de Formatos</b>	<b>6 Expedientes</b>				
<b>Cantidad Global de Datos Personales</b>	<b>24 Datos Personales Tratados</b>				
<b>Quien suministra</b>	El ciudadano del Municipio de Marín, N.L.				
<b>Cómo suministra</b>	Directamente - Presencial				
<b>Forma de obtención de datos</b>	Constancias				
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>
	<b>Tipo de Soporte</b>	SI			
<b>Descripción</b>	Formato establecido para hacer la constancia				



<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	INE, COMPROBANTE DE DOMICILIO				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE OFICINA DEL SINDICO MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el ciudadano lo autoriza					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						

<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SINDICO DEL AYUNTAMIENO			<b>Tiempo</b>	INDEFINIDO	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Increment al	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SINDICATURA MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR						
<b>I.- Nombre del sistema:</b>		CONSTANCIA DE BUENA CONDUCTA				
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>						
Administrador Responsable						
<b>Nombre:</b>	Rosalba Carolina González Caballero	<b>Cargo:</b>	SINDICO DEL AYUNTAMIENTO			
Encargado						
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA			
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>						
<b>Objetivo:</b>	Brindar un documento a los elementos de seguridad pública acreditando su buena conducta en la corporación.					
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.					
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)					
	<b>Dato Personal</b>		<b>Idoneidad</b>			
	Nombre		Para la identificación			
	Domicilio		Para la identificación			
	Nombre de los Testigos		Para constar y certificar dicho tramite			
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>					
<b>Volumen de Formatos</b>	<b>0 Expedientes</b>					
<b>Cantidad Global de Datos Personales</b>	<b>0 Datos Personales Tratados</b>					
<b>Quien suministra</b>	El ciudadano del Municipio de Marín, N.L.					
<b>Cómo suministra</b>	Directamente - Presencial					
<b>Forma de obtención de datos</b>	Constancias					
<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para hacer la constancia			
<b>Documentos Adjuntos con protección de datos personales</b>		INE, COMPROBANTE DE DOMICILIO Y EL INE DE 2 TESTIGOS				

	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE OFICINA DEL SINDICO MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	Obtención, conservación y utilización.					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el ciudadano lo autoriza					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO

<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SINDICO DEL AYUNTAMIENO			<b>Tiempo</b>	INDEFINIDO	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SINDICATURA MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR			
<b>I.- Nombre del sistema:</b>		CONSTANCIA AUTORIZACION DE MENOR	
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>			
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
<b>Administrador Responsable</b>			
<b>Nombre:</b>	Rosalba Carolina González Caballero	<b>Cargo:</b>	SINDICO DEL AYUNTAMIENTO
<b>Encargado</b>			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b>			
<b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Brindar un documento en el cual se autoriza que un menor salga del país con alguna otra persona que no sean sus padres.		
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.		
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)		
	<b>Dato Personal</b>	<b>Idoneidad</b>	
	Nombre del menor	Para la identificación	
	Nombre de los padres	Para la identificación	
	Domicilio actual	Para la identificación	
	Teléfono	Para la identificación	
	Domicilio a donde viajará	Para constar y certificar dicho tramite	
	Nombre de las personas que viajaran con el menor	Para constar y certificar dicho tramite	
	Nombre de los Testigos	Para constar y certificar dicho tramite	
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>7 Datos</b>		
<b>Volumen de Formatos</b>	<b>0 Expedientes</b>		
<b>Cantidad Global de Datos Personales</b>	<b>0 Datos Personales Tratados</b>		
<b>Quien suministra</b>	El ciudadano del Municipio de Marín, N.L.		
<b>Cómo suministra</b>	Directamente - Presencial		
<b>Forma de obtención de datos</b>	Constancias		

<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para hacer la constancia			
	<b>Documentos Adjuntos con protección de datos personales</b>		<ul style="list-style-type: none"> <li>• Acta de nacimiento del menor</li> <li>• INE de los padres</li> <li>• Comprobante de domicilio</li> <li>• INE de 2 testigos</li> </ul>			
	<b>Características del lugar donde se resguardan</b>		ARCHIVERO DE OFICINA DEL SINDICO MUNICIPAL			
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b> <b>VII.- Resguardo de los Sistemas</b> <b>XII.- Medidas de seguridad aplicadas a las instalaciones</b> <b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el ciudadano lo autoriza					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						

<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SINDICO DEL AYUNTAMIENO			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Increment al	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						



## SINDICATURA MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR			
<b>I.- Nombre del sistema:</b>		CONSTANCIA DE EXHUMACIÓN	
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>			
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
<b>Administrador Responsable</b>			
<b>Nombre:</b>	Rosalba Carolina González Caballero	<b>Cargo:</b>	SINDICO DEL AYUNTAMIENTO
<b>Encargado</b>			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b>			
<b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Brindar un documento en el cual se autoriza que un menor salga del país con alguna otra persona que no sean sus padres.		
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.		
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)		
	Dato Personal	Idoneidad	
	Nombre del familiar	Para la identificación	
	Domicilio	Para la identificación	
	Nombre y fecha de fallecimiento del difunto	Para constar y certificar dicho tramite	
	Nombre del Panteón	Para constar y certificar dicho tramite	
	Numero de Fila y Lote donde esta Sepultado	Para constar y certificar dicho tramite	
	Lugar a donde será trasladado	Para constar y certificar dicho tramite	
	Nombre de 2 Testigos y dirección	Para constar y certificar dicho tramite	
	<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>10 Datos</b>	
<b>Volumen de Formatos</b>	<b>3 Expedientes</b>		
<b>Cantidad Global de Datos Personales</b>	<b>30 Datos Personales Tratados</b>		
<b>Quien suministra</b>	Familiar Directo del difunto sepultado en el Panteón Municipal		
<b>Cómo suministra</b>	Directamente - Presencial		
<b>Forma de obtención de datos</b>	Constancias		

<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para hacer la constancia			
	<b>Documentos Adjuntos con protección de datos personales</b>		<ul style="list-style-type: none"> <li>• INE del solicitante (familiar directo),</li> <li>• INE de 2 testigos</li> <li>• Escritura de lote de panteón,</li> <li>• Copia de acta de función</li> <li>• Lugar a donde serán trasladados los restos,</li> <li>• Pago de derechos ante tesorería Municipal</li> </ul>			
	<b>Características del lugar donde se resguardan</b>		ARCHIVERO DE OFICINA DEL SINDICO MUNICIPAL			
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b> <b>VII.- Resguardo de los Sistemas</b> <b>XII.- Medidas de seguridad aplicadas a las instalaciones</b> <b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el ciudadano lo autoriza					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					

almacenamiento física						
<b>Acceso a las instalaciones</b>						
Seguridad perimetral exterior: <b>SI SE CUENTA</b>						
Seguridad perimetral interior: <b>SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						
Soporte de la bitácora:	Físico	SI	Electrónico	NO	Otro:	NO
Lugar de almacenamiento:	ARCHIVERO OFICINA			Tiempo	3 AÑOS	
Como se asegura la integridad:	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
Datos que se registran: fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
Soporte del registro:	Físico	SI	Electrónico	USB	Otro:	NO
Lugar de almacenamiento:	OFICINA SINDICO DEL AYUNTAMIENO			Tiempo	3 AÑOS	
Como se asegura la integridad:	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
Tipo de respaldo:	Completo	NO	Diferencial	NO	Increment al	SI
Medios para almacenar copias de seguridad	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia		Si	X	NO		
Se realizan pruebas de eficiencia		Si	X	NO		
Se cuenta con un sitio redundante		Si	X	NO		
Procedimiento	NO APLICA					
Equipo	NO APLICA					
Personal	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
Datos del sistema que será cancelado: NO APLICA						
Denominación:	NO APLICA					
Motivos:	NO APLICA					
Plazos y condiciones para el bloqueo del sistema:						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: NO APLICA						
Procedimiento para la supresión y periodo de conservación del sistema: NO APLICA						
Mecanismos para la supresión del sistema: En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SINDICATURA MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR						
<b>I.- Nombre del sistema:</b>		CONSTANCIA DE IDENTIDAD				
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>						
Administrador Responsable						
<b>Nombre:</b>	Rosalba Carolina González Caballero	<b>Cargo:</b>	SINDICO DEL AYUNTAMIENTO			
Encargado						
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA			
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>						
<b>Objetivo:</b>	Brindar un documento que avala la circunstancia en que se encuentra un individuo cuando no cuenta con una identificación oficial					
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.					
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)					
	<b>Dato Personal</b>		<b>Idoneidad</b>			
	Nombre		Para la identificación			
	Domicilio		Para la identificación			
	Edad		Para constar y certificar dicho tramite			
	Fecha y Lugar de Nacimiento		Para constar y certificar dicho tramite			
	Nombre de los Padres		Para constar y certificar dicho tramite			
	Nombre de Testigos		Para constar y certificar dicho tramite			
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>7 Datos</b>					
<b>Volumen de Formatos</b>	<b>80 Expedientes</b>					
<b>Cantidad Global de Datos Personales</b>	<b>560 Datos Personales Tratados</b>					
<b>Quien suministra</b>	Ciudadano del Municipio de Marín, N.L.					
<b>Cómo suministra</b>	Directamente - Presencial					
<b>Forma de obtención de datos</b>	Constancias					
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	SI
	<b>Tipo de Soporte</b>		Formato establecido para hacer la constancia			

<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	<ul style="list-style-type: none"> <li>• Acta de nacimiento</li> <li>• comprobante de domicilio</li> <li>• fotografía tamaño infantil</li> <li>• INE de 2 testigos</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE OFICINA DEL SINDICO MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el ciudadano lo autoriza					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						

<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SINDICO DEL AYUNTAMIENO			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SINDICATURA MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR					
<b>I.- Nombre del sistema:</b>		CONSTANCIA DE NO AFECTACIONES A VIA PÚBLICA			
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>					
Administrador Responsable					
<b>Nombre:</b>	Rosalba Carolina González Caballero	<b>Cargo:</b>	SINDICO DEL AYUNTAMIENTO		
Encargado					
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA		
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>					
<b>Objetivo:</b>	Brindar un documento para hacer constar que los nuevos proyectos no tienen afectaciones sobre las vías públicas actuales y/o futura, instalaciones o estructuras en propiedad del ayuntamiento según los programas de ordenamiento y/o desarrollo vigente y demás instrumento				
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.				
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)				
	<b>Dato Personal</b>		<b>Idoneidad</b>		
	Nombre		Para la identificación		
	Domicilio		Para la identificación		
	Nombre de Topografo		Para constar y certificar dicho tramite		
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>				
<b>Volumen de Formatos</b>	<b>9 Expedientes</b>				
<b>Cantidad Global de Datos Personales</b>	<b>27 Datos Personales Tratados</b>				
<b>Quien suministra</b>	Ciudadano del Municipio de Marín, N.L.				
<b>Cómo suministra</b>	Directamente - Presencial				
<b>Forma de obtención de datos</b>	Constancias				
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b> SI
<b>Tipo de Soporte</b>	<b>Descripción</b>		Formato establecido para hacer la constancia		

<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	<ul style="list-style-type: none"> <li>• Oficio de solicitud</li> <li>• escrituras de terreno</li> <li>• INE del propietario</li> <li>• plano topográfico</li> <li>• INE de apoderado</li> <li>• Cedula profesional de quien realizo el levantamiento topográfico</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE OFICINA DEL SINDICO MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	Obtención, conservación y utilización.					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b> <b>VII.- Resguardo de los Sistemas</b> <b>XII.- Medidas de seguridad aplicadas a las instalaciones</b> <b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el ciudadano lo autoriza					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						



<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SINDICO DEL AYUNTAMIENO			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SINDICATURA MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR					
<b>I.- Nombre del sistema:</b>		CONSTANCIA DE SEPARACION			
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>					
Administrador Responsable					
<b>Nombre:</b>	Rosalba Carolina González Caballero	<b>Cargo:</b>	SINDICO DEL AYUNTAMIENTO		
Encargado					
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA		
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>					
<b>Objetivo:</b>	Brindar un documento cuando una persona se separa de otra en una relación.				
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.				
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)				
	<b>Dato Personal</b>		<b>Idoneidad</b>		
	Nombre		Para la identificación		
	Domicilio		Para la identificación		
	Nombre de hijos(as)		Para la identificación		
	Fecha de Separacion		Para constar y certificar dicho tramite		
	Nombre de Testigos		Para constar y certificar dicho tramite		
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>5 Datos</b>				
<b>Volumen de Formatos</b>	<b>1 Expedientes</b>				
<b>Cantidad Global de Datos Personales</b>	<b>5 Datos Personales Tratados</b>				
<b>Quien suministra</b>	Ciudadano del Municipio de Marín, N.L.				
<b>Cómo suministra</b>	Directamente - Presencial				
<b>Forma de obtención de datos</b>	Constancias				
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>
	<b>Tipo de Soporte</b>	SI			
<b>Forma de obtención de datos</b>	<b>Descripción</b>		Formato establecido para hacer la constancia		

<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	<ul style="list-style-type: none"> <li>• INE</li> <li>• Comprobante de domicilio</li> <li>• INE de 2 testigos</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE OFICINA DEL SINDICO MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el ciudadano lo autoriza					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						

<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SINDICO DEL AYUNTAMIENO			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SINDICATURA MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR						
<b>I.- Nombre del sistema:</b>		CONSTANCIA DE TUTOR				
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>						
Administrador Responsable						
<b>Nombre:</b>	Rosalba Carolina González Caballero	<b>Cargo:</b>	SINDICO DEL AYUNTAMIENTO			
Encargado						
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA			
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>						
<b>Objetivo:</b>	Brindar un documento que se expide cuando una persona es responsable de un menor.					
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.					
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)					
	<b>Dato Personal</b>		<b>Idoneidad</b>			
	Nombre del Responsable		Para la identificación			
	Nombre del Menor		Para la identificación			
	Nombre de hijos(as)		Para la identificación			
	Nombre de Testigos		Para constar y certificar dicho tramite			
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>					
<b>Volumen de Formatos</b>	<b>8 Expedientes</b>					
<b>Cantidad Global de Datos Personales</b>	<b>24 Datos Personales Tratados</b>					
<b>Quien suministra</b>	Ciudadano del Municipio de Marín, N.L.					
<b>Cómo suministra</b>	Directamente - Presencial					
<b>Forma de obtención de datos</b>	Constancias					
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para hacer la constancia			
<b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>		<ul style="list-style-type: none"> <li>INE</li> <li>Acta de nacimiento del menor</li> <li>Comprobante de domicilio</li> <li>INE de 2 testigos</li> </ul>			

	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE OFICINA DEL SINDICO MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b> <b>VII.- Resguardo de los Sistemas</b> <b>XII.- Medidas de seguridad aplicadas a las instalaciones</b> <b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el ciudadano lo autoriza					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	

<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SINDICO DEL AYUNTAMIENO			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Increment al	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SINDICATURA MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR						
<b>I.- Nombre del sistema:</b>		CONSTANCIA DE RESIDENCIA				
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>						
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>						
<b>Administrador Responsable</b>						
<b>Nombre:</b>	Rosalba Carolina González Caballero	<b>Cargo:</b>	SINDICO DEL AYUNTAMIENTO			
<b>Encargado</b>						
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA			
<b>IV.- Inventario de datos personales</b>						
<b>V.- Estructura y descripción de los sistemas</b>						
<b>Objetivo:</b>	Brindar un documento que se expide en donde vive la persona que lo solicita.					
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.					
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)					
	<b>Dato Personal</b>	<b>Idoneidad</b>				
	Nombre	Para la identificación				
	Domicilio	Para la identificación				
	Nombre de Testigos	Para constar y certificar dicho tramite				
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>					
<b>Volumen de Formatos</b>	<b>15 Expedientes</b>					
<b>Cantidad Global de Datos Personales</b>	<b>45 Datos Personales Tratados</b>					
<b>Quien suministra</b>	Ciudadano del Municipio de Marín, N.L.					
<b>Cómo suministra</b>	Directamente - Presencial					
<b>Forma de obtención de datos</b>	Constancias					
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para hacer la constancia			
<b>Tipo de Soporte</b>	<b>Documentos Adjuntos con protección de datos personales</b>		<ul style="list-style-type: none"> <li>INE</li> <li>Comprobante de domicilio</li> <li>INE de 2 testigos</li> </ul>			



	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE OFICINA DEL SINDICO MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b> <b>VII.- Resguardo de los Sistemas</b> <b>XII.- Medidas de seguridad aplicadas a las instalaciones</b> <b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el ciudadano lo autoriza					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	

<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SINDICO DEL AYUNTAMIENO			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Increment al	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## TESORERÍA MUNICIPAL

UNIDAD ADMINISTRATIVA: DIRECCIÓN DE INGRESOS Y EGRESOS			
<b>I.- Nombre del sistema:</b>	ALTA DE PADRON DE PROVEEDORES		
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
<b>Administrador Responsable</b>			
<b>Nombre:</b>	Mario Gutiérrez González	<b>Cargo:</b>	TESORERO MUNICIPAL
<b>Usuario Responsable 1</b>			
<b>Nombre:</b>	Oscar Uriel Saucedá Fresnillo	<b>Cargo:</b>	ASISTENTE
<b>Usuario Responsable 2</b>			
<b>Nombre:</b>	Wendy Guadalupe Mejía Estrada	<b>Cargo:</b>	ASISTENTE
<b>Encargado</b>			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Tener un control de los expedientes de los proveedores que nos brindan servicio al Gobierno Municipal de Marín, N.L.y Formar parte de los requisitos para ingresar como proveedores, para integrar su expediente como proveedor y sirva como constancia ante la Auditoria Superior del Estado de Nuevo León.		
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.		
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)		
	<b>Dato Personal</b>	<b>Idoneidad</b>	
	Nombre	Para la identificación	
	Domicilio	Para la identificación	
	Teléfono	Para la identificación	
	RFC	Para la identificación	
	CURP	Para la identificación	
	Información Fiscal	Para la identificación	
	Ingresos y Egresos	Para la identificación	
Seguros y Fianzas	Para la identificación		
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>8 Datos</b>		
<b>Volumen de Formatos</b>	<b>440 Expedientes</b>		

<b>Cantidad Global de Datos Personales</b>	<b>3,520 Datos Personales Tratados</b>					
<b>Quien suministra</b>	El proveedor.					
<b>Cómo suministra</b>	Directamente - Presencial					
<b>Forma de obtención de datos</b>	Formulario					
<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	SI	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para hacer el pago			
	<b>Documentos Adjuntos con protección de datos personales</b>		<ul style="list-style-type: none"> <li>• INE</li> <li>• CONSTANCIA DE SITUACION FISCAL, ACTA CONSTITUTIVA DE LA EMPRESA, COMPROBANTE DE DOMICILIO</li> </ul>			
	<b>Características del lugar donde se resguardan</b>		ARCHIVERO DE TESORERIA MUNICIPAL			
<b>Participación en el ciclo de vida del dato personal</b>	Obtención, conservación y utilización.					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	SI	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder. Únicamente se sube la información a la base de datos de Transparencia y cuando lo solicita Auditoría del Estado					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el Auditor lo Solicita					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	SI	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	SI	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					

<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	si	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA TESORERIA MPAL			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## TESORERÍA MUNICIPAL

UNIDAD ADMINISTRATIVA: DIRECCIÓN DE INGRESOS Y EGRESOS						
<b>I.- Nombre del sistema:</b>		TRANSFERENCIA ELECTRONICAS				
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>						
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>						
<b>Administrador Responsable</b>						
<b>Nombre:</b>	Mario Gutiérrez González	<b>Cargo:</b>	TESORERO MUNICIPAL			
<b>Usuario Responsable 1</b>						
<b>Nombre:</b>	Oscar Uriel Saucedá Fresnillo	<b>Cargo:</b>	ASISTENTE			
<b>Usuario Responsable 2</b>						
<b>Nombre:</b>	Wendy Guadalupe Mejía Estrada	<b>Cargo:</b>	ASISTENTE			
<b>Encargado</b>						
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA			
<b>IV.- Inventario de datos personales</b>						
<b>V.- Estructura y descripción de los sistemas</b>						
<b>Objetivo:</b>	Tener un control de los expedientes de las transferencias electrónicas					
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.					
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)					
	<b>Dato Personal</b>	<b>Idoneidad</b>				
	Razón Social	Para la identificación				
	Domicilio	Para la identificación				
	Teléfono	Para la identificación				
	Factura de Pago	Para la identificación				
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>4 Datos</b>					
<b>Volumen de Formatos</b>	<b>4,500 Expedientes</b>					
<b>Cantidad Global de Datos Personales</b>	<b>18,000 Datos Personales Tratados</b>					
<b>Quien suministra</b>	El proveedor.					
<b>Cómo suministra</b>	Directamente - Presencial					
<b>Forma de obtención de datos</b>	Formulario					
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	SI	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para hacer el pago			

<b>Tipo de Soporte Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	<ul style="list-style-type: none"> <li>• INE</li> <li>• CONSTANCIA DE SITUACION FISCAL, ACTA CONSTITUTIVA DE LA EMPRESA, COMPROBANTE DE DOMICILIO</li> <li>• FACTURA PARA REALIZAR EL PAGO</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE TESORERIA MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	Obtención, conservación y utilización.					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	SI	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder. Únicamente se sube la información a la base de datos de Transparencia y cuando lo solicita Auditoria del Estado					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el Auditor lo Solicita					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	SI	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	SI	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						

<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	si	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA TESORERIA MPAL			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Increment al	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						



## TESORERÍA MUNICIPAL

UNIDAD ADMINISTRATIVA: DIRECCIÓN DE INGRESOS Y EGRESOS			
<b>I.- Nombre del sistema:</b>		CHEQUES NOMINATIVOS	
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>			
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
<b>Administrador Responsable</b>			
<b>Nombre:</b>	Mario Gutiérrez González	<b>Cargo:</b>	TESORERO MUNICIPAL
<b>Usuario Responsable 1</b>			
<b>Nombre:</b>	Oscar Uriel Saucedá Fresnillo	<b>Cargo:</b>	ASISTENTE
<b>Usuario Responsable 2</b>			
<b>Nombre:</b>	Wendy Guadalupe Mejía Estrada	<b>Cargo:</b>	ASISTENTE
<b>Encargado</b>			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b>			
<b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Tener un control de los expedientes de los cheques nominativos		
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.		
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)		
	<b>Dato Personal</b>	<b>Idoneidad</b>	
	Nombre	Para la identificación	
	Domicilio	Para la identificación	
	Teléfono	Para la identificación	
	Factura de Pago	Para la identificación	
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>4 Datos</b>		
<b>Volumen de Formatos</b>	<b>3,000 Expedientes</b>		
<b>Cantidad Global de Datos Personales</b>	<b>12,000 Datos Personales Tratados</b>		
<b>Quien suministra</b>	El proveedor.		
<b>Cómo suministra</b>	Directamente - Presencial		

<b>Forma de obtención de datos</b>	Formulario					
<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	SI	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para hacer la constancia			
	<b>Documentos Adjuntos con protección de datos personales</b>		<ul style="list-style-type: none"> <li>• INE</li> <li>• CONSTANCIA DE SITUACION FISCAL, ACTA CONSTITUTIVA DE LA EMPRESA, COMPROBANTE DE DOMICILIO</li> <li>• FACTURA PARA REALIZAR EL PAGO</li> </ul>			
	<b>Características del lugar donde se resguardan</b>		ARCHIVERO DE TESORERIA MUNICIPAL			
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	SI	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder. Únicamente se sube la información a la base de datos de Transparencia y cuando lo solicita Auditoria del Estado					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el Auditor lo Solicita					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	SI	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	SI	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					

almacenamiento física						
<b>Acceso a las instalaciones</b>						
Seguridad perimetral exterior: <b>SI SE CUENTA</b>						
Seguridad perimetral interior: <b>SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						
Soporte de la bitácora:	Físico	SI	Electrónico	SI	Otro:	NO
Lugar de almacenamiento:	ARCHIVERO OFICINA			Tiempo	3 AÑOS	
Como se asegura la integridad:	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
Datos que se registran: fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
Soporte del registro:	Físico	SI	Electrónico	USB	Otro:	NO
Lugar de almacenamiento:	OFICINA TESORERIA MPAL			Tiempo	3 AÑOS	
Como se asegura la integridad:	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
Tipo de respaldo:	Completo	NO	Diferencial	NO	Incremental	SI
Medios para almacenar copias de seguridad	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia	Si	X	NO			
Se realizan pruebas de eficiencia	Si	X	NO			
Se cuenta con un sitio redundante	Si	X	NO			
Procedimiento	NO APLICA					
Equipo	NO APLICA					
Personal	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
Datos del sistema que será cancelado: NO APLICA						
Denominación:	NO APLICA					
Motivos:	NO APLICA					
Plazos y condiciones para el bloqueo del sistema:						
Medidas de seguridad para el bloqueo y posterior supresión del sistema: NO APLICA						
Procedimiento para la supresión y periodo de conservación del sistema: NO APLICA						
Mecanismos para la supresión del sistema: En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## TESORERÍA MUNICIPAL

UNIDAD ADMINISTRATIVA: DIRECCIÓN DE INGRESOS Y EGRESOS					
<b>I.- Nombre del sistema:</b>		LICENCIAS DE CONDUCIR			
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>					
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>					
<b>Administrador Responsable</b>					
<b>Nombre:</b>	Mario Gutiérrez González	<b>Cargo:</b>	TESORERO MUNICIPAL		
<b>Usuario Responsable 1</b>					
<b>Nombre:</b>	Oscar Uriel Saucedá Fresnillo	<b>Cargo:</b>	ASISTENTE		
<b>Usuario Responsable 2</b>					
<b>Nombre:</b>	Wendy Guadalupe Mejía Estrada	<b>Cargo:</b>	ASISTENTE		
<b>Encargado</b>					
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA		
<b>IV.- Inventario de datos personales</b>					
<b>V.- Estructura y descripción de los sistemas</b>					
<b>Objetivo:</b>	Tener un control de los expedientes de las licencias de conducir que se expiden por primera vez				
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.				
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)				
	<b>Dato Personal</b>	<b>Idoneidad</b>			
	Nombre	Para la identificación			
	Domicilio	Para la identificación			
	Teléfono	Para la identificación			
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>				
<b>Volumen de Formatos</b>	<b>20 Expedientes</b>				
<b>Cantidad Global de Datos Personales</b>	<b>60 Datos Personales Tratados</b>				
<b>Quien suministra</b>	El proveedor.				
<b>Cómo suministra</b>	Directamente - Presencial				
<b>Forma de obtención de datos</b>	Formulario				
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>
<b>Tipo de Soporte</b>	<b>Descripción</b>		Formato establecido para hacer la constancia		

<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	<ul style="list-style-type: none"> <li>• INE</li> <li>• COMPROBANTE DE DOMICILIO</li> <li>• ACTA DE NACIMIENTO</li> <li>• EXAMEN APROBADO POR SEGURIDAD PUBLICA MPAL</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE TESORERIA MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	Obtención, conservación y utilización.					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el Auditor lo Solicita					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						

<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA TESORERIA MPAL			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Increment al	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## TESORERÍA MUNICIPAL

UNIDAD ADMINISTRATIVA: DIRECCIÓN DE INGRESOS Y EGRESOS					
<b>I.- Nombre del sistema:</b>		RECIBO DE EGRESOS (APOYOS)			
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>					
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>					
<b>Administrador Responsable</b>					
<b>Nombre:</b>	Mario Gutiérrez González	<b>Cargo:</b>	TESORERO MUNICIPAL		
<b>Usuario Responsable 1</b>					
<b>Nombre:</b>	Oscar Uriel Saucedá Fresnillo	<b>Cargo:</b>	ASISTENTE		
<b>Usuario Responsable 2</b>					
<b>Nombre:</b>	Wendy Guadalupe Mejía Estrada	<b>Cargo:</b>	ASISTENTE		
<b>Encargado</b>					
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA		
<b>IV.- Inventario de datos personales</b>					
<b>V.- Estructura y descripción de los sistemas</b>					
<b>Objetivo:</b>	Tener un control de los expedientes de egresos monetarios (apoyos)				
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.				
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)				
	<b>Dato Personal</b>	<b>Idoneidad</b>			
	Nombre	Para la identificación			
	Domicilio	Para la identificación			
	Teléfono	Para la identificación			
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>				
<b>Volumen de Formatos</b>	<b>20 Expedientes</b>				
<b>Cantidad Global de Datos Personales</b>	<b>60 Datos Personales Tratados</b>				
<b>Quien suministra</b>	El ciudadano de Marín, N.L.				
<b>Cómo suministra</b>	Directamente - Presencial				
<b>Forma de obtención de datos</b>	Formulario				
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>
<b>Tipo de Soporte</b>	<b>Descripción</b>		Formato establecido para hacer la constancia		

<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	• INE				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE TESORERIA MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si el Auditor lo Solicita					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						



<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA TESORERIA MPAL			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## TESORERÍA MUNICIPAL

UNIDAD ADMINISTRATIVA: DIRECCIÓN DE INGRESOS Y EGRESOS					
<b>I.- Nombre del sistema:</b>		PREDIAL			
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>					
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>					
<b>Administrador Responsable</b>					
<b>Nombre:</b>	Mario Gutiérrez González	<b>Cargo:</b>	TESORERO MUNICIPAL		
<b>Usuario Responsable 1</b>					
<b>Nombre:</b>	Oscar Uriel Saucedá Fresnillo	<b>Cargo:</b>	ASISTENTE		
<b>Usuario Responsable 2</b>					
<b>Nombre:</b>	Wendy Guadalupe Mejía Estrada	<b>Cargo:</b>	ASISTENTE		
<b>Encargado</b>					
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA		
<b>IV.- Inventario de datos personales</b>					
<b>V.- Estructura y descripción de los sistemas</b>					
<b>Objetivo:</b>	Tener un control de los expedientes de pago del impuesto predial				
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.				
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)				
	<b>Dato Personal</b>	<b>Idoneidad</b>			
	Nombre	Para la identificación			
	Domicilio	Para la identificación			
	Teléfono	Para la identificación			
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>				
<b>Volumen de Formatos</b>	<b>1,200 Expedientes</b>				
<b>Cantidad Global de Datos Personales</b>	<b>3,600 Datos Personales Tratados</b>				
<b>Quien suministra</b>	El ciudadano de Marín, N.L.				
<b>Cómo suministra</b>	Directamente - Presencial				
<b>Forma de obtención de datos</b>	Formulario				
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	SI	<b>Vía Telefónica</b> NO
<b>Tipo de Soporte</b>	<b>Descripción</b>		Formato establecido para hacer el proceso del pago		

<b>Forma de obtención de datos</b>						
	<b>Documentos Adjuntos con protección de datos personales</b>	NINGUNO SOLO SE DEJA COPIA DEL RECIBO DE PAGO				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE TESORERIA MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	No aplica					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si se solicita por medio de Transparencia el ciudadano					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						

<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA TESORERIA MPAL			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Increment al	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia		Si	X	NO		
Se realizan pruebas de eficiencia		Si	X	NO		
Se cuenta con un sitio redundante		Si	X	NO		
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## ORGANO INTERNO DE CONTROL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DEL ORGANO INTERNO DE CONTROL					
<b>I.- Nombre del sistema:</b>		PROCEDIMIENTO DE RESPONSABILIDAD ADMINISTRATIVA			
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>					
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>					
<b>Administrador Responsable</b>					
<b>Nombre:</b>	Julio Cesar Molina González	<b>Cargo:</b>	TITULAR DEL ORGANO INTERNO DE CONTROL		
<b>Usuario Responsable 1</b>					
<b>Nombre:</b>	Maribel Pérez González	<b>Cargo:</b>	Autoridad Sustanciadora del Órgano Interno de Control		
<b>Encargado</b>					
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA		
<b>IV.- Inventario de datos personales</b>					
<b>V.- Estructura y descripción de los sistemas</b>					
<b>Objetivo:</b>	Sancionar a los servidores públicos que incurran en responsabilidades administrativas. Vigilar que el actuar de los servidores públicos este apegado al marco legal y en caso de detectar violaciones iniciar investigaciones para determinar las responsabilidades administrativas y sancionar a los imputados.				
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.				
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)				
	<b>Dato Personal</b>	<b>Idoneidad</b>			
	Nombre	Para la identificación			
	Domicilio	Para la identificación			
	Teléfono	Para la identificación			
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>				
<b>Volumen de Formatos</b>	<b>11 Expedientes</b>				
<b>Cantidad Global de Datos Personales</b>	<b>33 Datos Personales Tratados</b>				
<b>Quien suministra</b>	El ciudadano de Marín, N.L.				
<b>Cómo suministra</b>	Directamente - Presencial				
<b>Forma de obtención de datos</b>	Formulario				
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	SI	<b>Vía Telefónica</b> NO
<b>Tipo de Soporte</b>	<b>Descripción</b>		Expediente sancionador		

<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	DOCUMENTOS COMPROBATORIOS PARA DICHO PROCESO				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO ORGANO INTERNO DE CONTROL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	No aplica					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si se solicita por medio de Transparencia el ciudadano					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso,					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión del Presidente Mpal y Tribunales					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						

<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA ORGANO INTERNO DE CONTROL			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## UNIDAD DE TRANSPARENCIA

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR UNIDAD DE TRANSPARENCIA					
<b>I.- Nombre del sistema:</b>	SOLICITUDES DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN DE DATOS PERSONALES (ARCO)				
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>					
<b>Administrador Responsable</b>					
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA		
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>					
<b>Objetivo:</b>	Tener un control de los expedientes de las Solicitudes de Acceso, Rectificación, Cancelación y Oposición de Datos Personales (Arco) que nos solicitan al Gobierno Municipal de Marín, N.L. Formar parte de los requisitos para requerir Solicitudes de Acceso, Rectificación, Cancelación y Oposición de Datos Personales (Arco), para integrar su expediente y sirva como constancia ante el Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales (INFONL) y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)				
<b>Fundamento Legal:</b>	Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.				
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)				
	<b>Dato Personal</b>	<b>Idoneidad</b>			
	Nombre	Para la identificación			
	Domicilio	Para la identificación			
	Teléfono	Para la identificación			
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>				
<b>Volumen de Formatos</b>	<b>11 Expedientes</b>				
<b>Cantidad Global de Datos Personales</b>	<b>33 Datos Personales Tratados</b>				
<b>Quien suministra</b>	El ciudadano que lo solicite				
<b>Cómo suministra</b>	Directamente - Presencial				
<b>Forma de obtención de datos</b>	Formulario				
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	SI	<b>Vía Telefónica</b> NO
<b>Tipo de Soporte</b>	<b>Descripción</b>		Expediente ARCO		



<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	DOCUMENTOS COMPROBATORIOS PARA DICHO PROCESO				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE UNIDAD DE TRANSPARENCIA				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	No aplica					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si se solicita por medio de Transparencia el ciudadano					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso,					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión del Presidente Mpal y Tribunales					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						

<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA UNIDAD DE TRANSPARENCIA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIF MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DIF MUNICIPAL													
<b>I.- Nombre del sistema:</b>		COMEDOR MIXTO											
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>													
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>													
<b>Administrador Responsable</b>													
<b>Nombre:</b>	Gloria Paulina Mendoza Gutierrez	<b>Cargo:</b>	SECRETARIA										
<b>Encargado</b>													
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA										
<b>IV.- Inventario de datos personales</b>													
<b>V.- Estructura y descripción de los sistemas</b>													
<b>Objetivo:</b>	Tener un control de los expedientes de información que se solicita a los beneficiarios.												
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.												
<b>Datos Personales que se encuentran en el sistema:</b>	<p style="text-align: center;"><b>ORDINARIOS</b> (Identificativos)</p> <table border="1" style="width: 100%; border-collapse: collapse; margin: 5px 0;"> <thead> <tr> <th style="width: 50%; padding: 5px;">Dato Personal</th> <th style="width: 50%; padding: 5px;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Nombre</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Domicilio</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Teléfono</td> <td style="padding: 5px;">Para la identificación</td> </tr> </tbody> </table>					Dato Personal	Idoneidad	Nombre	Para la identificación	Domicilio	Para la identificación	Teléfono	Para la identificación
Dato Personal	Idoneidad												
Nombre	Para la identificación												
Domicilio	Para la identificación												
Teléfono	Para la identificación												
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>												
<b>Volumen de Formatos</b>	<b>0 Expedientes</b>												
<b>Cantidad Global de Datos Personales</b>	<b>0 Datos Personales Tratados</b>												
<b>Quien suministra</b>	El ciudadano que lo solicite												
<b>Cómo suministra</b>	Directamente - Presencial												
<b>Forma de obtención de datos</b>	Formulario												
<b>Forma de obtención de datos</b>	Físico	SI	Electrónico	NO	Vía Telefónica	NO							
<b>Tipo de Soporte Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>		Expediente para el apoyo										
			<ul style="list-style-type: none"> <li>ESTUDIO SOCIOECONÓMICO (SE REALIZA AL SOLICITAR EL APOYO EN DIF MUNICIPAL)</li> <li>IDENTIFICACIÓN OFICIAL (INE)</li> </ul>										

		<ul style="list-style-type: none"> <li>• COMPROBANTE DE DOMICILIO (NO MAYOR A 3 MESES DE ANTIGÜEDAD)</li> <li>• CURP</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DEL DIF MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	No aplica					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si se solicita por medio de Transparencia el ciudadano					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso,					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						

<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DIF MUNICIPAL			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIF MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DIF MUNICIPAL													
<b>I.- Nombre del sistema:</b>		TRASLADOS											
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>													
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>													
Administrador Responsable													
<b>Nombre:</b>	Gloria Paulina Mendoza Gutierrez	<b>Cargo:</b>	SECRETARIA										
Encargado													
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA										
<b>IV.- Inventario de datos personales</b>													
<b>V.- Estructura y descripción de los sistemas</b>													
<b>Objetivo:</b>	Tener un control de los expedientes de información que se solicita a los beneficiarios.												
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.												
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos) <table border="1" style="width: 100%; margin-top: 5px;"> <thead> <tr> <th style="width: 50%;">Dato Personal</th> <th style="width: 50%;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td>Nombre</td> <td>Para la identificación</td> </tr> <tr> <td>Domicilio</td> <td>Para la identificación</td> </tr> <tr> <td>Teléfono</td> <td>Para la identificación</td> </tr> </tbody> </table>					Dato Personal	Idoneidad	Nombre	Para la identificación	Domicilio	Para la identificación	Teléfono	Para la identificación
Dato Personal	Idoneidad												
Nombre	Para la identificación												
Domicilio	Para la identificación												
Teléfono	Para la identificación												
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>												
<b>Volumen de Formatos</b>	<b>1,584 Expedientes</b>												
<b>Cantidad Global de Datos Personales</b>	<b>4,752 Datos Personales Tratados</b>												
<b>Quien suministra</b>	El ciudadano que lo solicite												
<b>Cómo suministra</b>	Directamente - Presencial												
<b>Forma de obtención de datos</b>	Formulario												
<b>Forma de obtención de datos</b>	Físico	SI	Electrónico	NO	Vía Telefónica	NO							
<b>Tipo de Soporte</b>	<b>Documentos Adjuntos con protección de datos personales</b>		Expediente para el apoyo										
<b>Forma de obtención de datos</b>			<ul style="list-style-type: none"> <li>COPIA TARJETA DE CITAS</li> <li>INE</li> </ul>										

	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DEL DIF MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b> <b>VII.- Resguardo de los Sistemas</b> <b>XII.- Medidas de seguridad aplicadas a las instalaciones</b> <b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	No aplica					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si se solicita por medio de Transparencia el ciudadano					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso,					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	

<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DIF MUNICIPAL			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						



## DIF MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DIF MUNICIPAL															
<b>I.- Nombre del sistema:</b>		BOLETOS DE AUTOBUS													
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>															
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>															
<b>Administrador Responsable</b>															
<b>Nombre:</b>	Gloria Paulina Mendoza Gutierrez	<b>Cargo:</b>	SECRETARIA												
<b>Encargado</b>															
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA												
<b>IV.- Inventario de datos personales</b>															
<b>V.- Estructura y descripción de los sistemas</b>															
<b>Objetivo:</b>	Tener un control de los expedientes de información que se solicita a los beneficiarios para su apoyo.														
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.														
<b>Datos Personales que se encuentran en el sistema:</b>	<table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr style="background-color: #f4a460;"> <th colspan="2" style="padding: 5px;"><b>ORDINARIOS</b> (Identificativos)</th> </tr> <tr style="background-color: #f4a460;"> <th style="width: 50%; padding: 5px;">Dato Personal</th> <th style="width: 50%; padding: 5px;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Nombre</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Domicilio</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Teléfono</td> <td style="padding: 5px;">Para la identificación</td> </tr> </tbody> </table>					<b>ORDINARIOS</b> (Identificativos)		Dato Personal	Idoneidad	Nombre	Para la identificación	Domicilio	Para la identificación	Teléfono	Para la identificación
<b>ORDINARIOS</b> (Identificativos)															
Dato Personal	Idoneidad														
Nombre	Para la identificación														
Domicilio	Para la identificación														
Teléfono	Para la identificación														
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>														
<b>Volumen de Formatos</b>	<b>17 Expedientes</b>														
<b>Cantidad Global de Datos Personales</b>	<b>51 Datos Personales Tratados</b>														
<b>Quien suministra</b>	El ciudadano que lo solicite														
<b>Cómo suministra</b>	Directamente - Presencial														
<b>Forma de obtención de datos</b>	Formulario														
<b>Forma de obtención de datos</b>	Físico	SI	Electrónico	NO	Vía Telefónica	NO									
<b>Tipo de Soporte</b>	Descripción		Expediente para el apoyo												

<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	<ul style="list-style-type: none"> <li>• COPIA TARJETA DE CITAS</li> <li>• INE</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DEL DIF MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	Obtención, conservación y utilización.					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	No aplica					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si se solicita por medio de Transparencia el ciudadano					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso,					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						

<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DIF MUNICIPAL			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia		Si	X	NO		
Se realizan pruebas de eficiencia		Si	X	NO		
Se cuenta con un sitio redundante		Si	X	NO		
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIF MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DIF MUNICIPAL						
<b>I.- Nombre del sistema:</b>		DESPENSA MUNICIPAL				
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>						
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>						
<b>Administrador Responsable</b>						
<b>Nombre:</b>	Gloria Paulina Mendoza Gutierrez	<b>Cargo:</b>	SECRETARIA			
<b>Encargado</b>						
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA			
<b>IV.- Inventario de datos personales</b>						
<b>V.- Estructura y descripción de los sistemas</b>						
<b>Objetivo:</b>	Tener un control de los expedientes de información que se solicita a los beneficiarios para su apoyo.					
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.					
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)					
	<b>Dato Personal</b>	<b>Idoneidad</b>				
	Nombre	Para la identificación				
	Domicilio	Para la identificación				
	Teléfono	Para la identificación				
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>					
<b>Volumen de Formatos</b>	<b>1,298 Expedientes</b>					
<b>Cantidad Global de Datos Personales</b>	<b>3,894 Datos Personales Tratados</b>					
<b>Quien suministra</b>	El ciudadano que lo solicite					
<b>Cómo suministra</b>	Directamente - Presencial					
<b>Forma de obtención de datos</b>	Formulario					
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	NO
	<b>Tipo de Soporte</b>	<b>Descripción</b>		Expediente para el apoyo		

<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	<ul style="list-style-type: none"> <li>• COPIA TARJETA DE CITAS</li> <li>• INE</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DEL DIF MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	Obtención, conservación y utilización.					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	No aplica					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si se solicita por medio de Transparencia el ciudadano					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso,					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						

<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DIF MUNICIPAL			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIF MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DIF MUNICIPAL													
<b>I.- Nombre del sistema:</b>		TERAPIA DE LENGUAJE											
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>													
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>													
<b>Administrador Responsable</b>													
<b>Nombre:</b>	Gloria Paulina Mendoza Gutierrez	<b>Cargo:</b>	SECRETARIA										
<b>Encargado</b>													
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA										
<b>IV.- Inventario de datos personales</b>													
<b>V.- Estructura y descripción de los sistemas</b>													
<b>Objetivo:</b>	Tener un control de los expedientes de información que se solicita a los beneficiarios para su apoyo.												
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.												
<b>Datos Personales que se encuentran en el sistema:</b>	<p style="text-align: center;"><b>ORDINARIOS</b> (Identificativos)</p> <table border="1" style="width: 100%; border-collapse: collapse; margin: 5px 0;"> <thead> <tr> <th style="width: 50%; padding: 5px;">Dato Personal</th> <th style="width: 50%; padding: 5px;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Nombre</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Domicilio</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Teléfono</td> <td style="padding: 5px;">Para la identificación</td> </tr> </tbody> </table>					Dato Personal	Idoneidad	Nombre	Para la identificación	Domicilio	Para la identificación	Teléfono	Para la identificación
Dato Personal	Idoneidad												
Nombre	Para la identificación												
Domicilio	Para la identificación												
Teléfono	Para la identificación												
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>												
<b>Volumen de Formatos</b>	<b>55 Expedientes</b>												
<b>Cantidad Global de Datos Personales</b>	<b>165 Datos Personales Tratados</b>												
<b>Quien suministra</b>	El ciudadano que lo solicite												
<b>Cómo suministra</b>	Directamente - Presencial												
<b>Forma de obtención de datos</b>	Formulario												
<b>Forma de obtención de datos</b>	Físico	SI	Electrónico	NO	Vía Telefónica	NO							
<b>Tipo de Soporte</b>	<b>Documentos Adjuntos con protección de datos personales</b>		<ul style="list-style-type: none"> <li>COMPROBANTE DE QUE ES UN ALUMNO ESCOLARIZADO</li> </ul>										

		<ul style="list-style-type: none"> <li>OFICIO DE PARTE DE LA ESCUELA DONDE SE EXPLIQUE BREVEMENTE QUE EL ALUMNO REQUIERE APOYO ESCOLAR</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DEL DIF MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	No aplica					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si se solicita por medio de Transparencia el ciudadano					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso,					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						



<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DIF MUNICIPAL			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia		Si	X	NO		
Se realizan pruebas de eficiencia		Si	X	NO		
Se cuenta con un sitio redundante		Si	X	NO		
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIF MUNICIPAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DIF MUNICIPAL													
<b>I.- Nombre del sistema:</b>		TERAPIA FISICA											
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>													
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>													
Administrador Responsable													
<b>Nombre:</b>	Gloria Paulina Mendoza Gutierrez	<b>Cargo:</b>	SECRETARIA										
Encargado													
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA										
<b>IV.- Inventario de datos personales</b>													
<b>V.- Estructura y descripción de los sistemas</b>													
<b>Objetivo:</b>	Tener un control de los expedientes de información que se solicita a los beneficiarios para su apoyo.												
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.												
<b>Datos Personales que se encuentran en el sistema:</b>	<p style="text-align: center;"><b>ORDINARIOS</b> (Identificativos)</p> <table border="1" style="width: 100%; border-collapse: collapse; margin: 5px 0;"> <thead> <tr> <th style="width: 50%; padding: 5px;">Dato Personal</th> <th style="width: 50%; padding: 5px;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Nombre</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Domicilio</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Teléfono</td> <td style="padding: 5px;">Para la identificación</td> </tr> </tbody> </table>					Dato Personal	Idoneidad	Nombre	Para la identificación	Domicilio	Para la identificación	Teléfono	Para la identificación
Dato Personal	Idoneidad												
Nombre	Para la identificación												
Domicilio	Para la identificación												
Teléfono	Para la identificación												
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>												
<b>Volumen de Formatos</b>	<b>220 Expedientes</b>												
<b>Cantidad Global de Datos Personales</b>	<b>660 Datos Personales Tratados</b>												
<b>Quien suministra</b>	El ciudadano que lo solicite												
<b>Cómo suministra</b>	Directamente - Presencial												
<b>Forma de obtención de datos</b>	Formulario												
<b>Forma de obtención de datos</b>	Físico	SI	Electrónico	NO	Vía Telefónica	NO							
<b>Tipo de Soporte</b>	<b>Documentos Adjuntos con protección de datos personales</b>		<ul style="list-style-type: none"> <li>INDICACIÓN DEL MÉDICO REHABILTADOR</li> <li>INE (COPIA)</li> <li>CURP (COPIA)</li> </ul>										

		<ul style="list-style-type: none"> <li>• COMPROBANTE DE DOMICILIO (NO MAYOR A 3 MESES DE ANTIGÜEDAD) (COPIA)</li> <li>• ACTA DE NACIMIENTO (COPIA)</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DEL DIF MUNICIPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	No aplica					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si se solicita por medio de Transparencia el ciudadano					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso,					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						

<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DIF MUNICIPAL			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SECRETARIA DEL AYUNTAMIENTO

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR			
<b>I.- Nombre del sistema:</b>		CONSTANCIA DE INGRESOS	
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>			
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
<b>Administrador Responsable</b>			
<b>Nombre:</b>	Julio Cesar Molina González	<b>Cargo:</b>	Secretario del Ayuntamiento
<b>Usuario Responsable 1</b>			
<b>Nombre:</b>	Alejandra Campos Salgado	<b>Cargo:</b>	ASISTENTE
<b>Encargado</b>			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b>			
<b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Generar una constancia donde podamos constar el ingreso que el ciudadano genera, ya que no cuenta con documentación que lo avale		
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.		
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)		
	<b>Dato Personal</b>	<b>Idoneidad</b>	
	Nombre	Para la identificación	
	Domicilio	Para la identificación	
	Teléfono	Para la notificación en su caso	
	<b>ECONOMICOS</b> (Identificativos)		
<b>Dato Personal</b>	<b>Idoneidad</b>		
Ingreso Mensual	Para la identificación		
Ocupación	Para la identificación		
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>5 Datos</b>		
<b>Volumen de Formatos</b>	<b>36 Expedientes</b>		
<b>Cantidad Global de Datos Personales</b>	<b>180 Datos Personales Tratados</b>		
<b>Quien suministra</b>	El ciudadano del Municipio de Marín, N.L.		
<b>Cómo suministra</b>	Directamente		
<b>Forma de obtención de datos</b>	Formato		

<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para llevar control			
	<b>Documentos Adjuntos con protección de datos personales</b>		(Solo se pide copia de su ine para incluir como constancia )			
	<b>Características del lugar donde se resguardan</b>		ARCHIVERO DE OFICINA DEL SECRETARIO DEL AYUNTAMIENTO			
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b> <b>VII.- Resguardo de los Sistemas</b> <b>XII.- Medidas de seguridad aplicadas a las instalaciones</b> <b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ningún persona ajena al deparamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si lo solicitan las máximas autoridades (Tesorería y auditoría del estado)					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección y solo se transfiere si lo solicitan las máximas autoridades (alcalde, secretario del ayuntamiento, tesorería y auditoría del estado.					
<b>Acceso a las instalaciones</b>						

<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SECRETARIA DEL AYUNTAMIENTO			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al termino de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SECRETARIA DEL AYUNTAMIENTO

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR						
<b>I.- Nombre del sistema:</b>		CONSTANCIA DE RECOMENDACION				
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>						
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>						
<b>Administrador Responsable</b>						
<b>Nombre:</b>	Julio Cesar Molina González	<b>Cargo:</b>	Secretario del Ayuntamiento			
<b>Usuario Responsable 1</b>						
<b>Nombre:</b>	Alejandra Campos Salgado	<b>Cargo:</b>	ASISTENTE			
<b>Encargado</b>						
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA			
<b>IV.- Inventario de datos personales</b>						
<b>V.- Estructura y descripción de los sistemas</b>						
<b>Objetivo:</b>	Generar una constancia donde podamos brindarle al ciudadano una recomendación para que pueda buscar trabajo					
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.					
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)					
	<b>Dato Personal</b>	<b>Idoneidad</b>				
	Nombre	Para la identificación				
	Domicilio	Para la identificación				
	Teléfono	Para la notificación en su caso				
	<b>ECONOMICOS</b> (Identificativos)					
<b>Dato Personal</b>	<b>Idoneidad</b>					
Ocupación	Para la identificación					
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>4 Datos</b>					
<b>Volumen de Formatos</b>	<b>20 Expedientes</b>					
<b>Cantidad Global de Datos Personales</b>	<b>80 Datos Personales Tratados</b>					
<b>Quien suministra</b>	El ciudadano del Municipio de Marín, N.L.					
<b>Cómo suministra</b>	Directamente					
<b>Forma de obtención de datos</b>	Formato					
<b>Forma de obtención de datos</b>	Físico	SI	Electrónico	NO	Vía Telefónica	SI



<b>Tipo de Soporte Forma de obtención de datos</b>	<b>Descripción</b>	Formato establecido para llevar control				
	<b>Documentos Adjuntos con protección de datos personales</b>	(Solo se pide copia de su ine para incluir como constancia )				
	<b>Características del lugar donde se resguardan</b>	ARCHIVERO DE OFICINA DEL SECRETARIO DEL AYUNTAMIENTO				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias VII.- Resguardo de los Sistemas XII.- Medidas de seguridad aplicadas a las instalaciones XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ningún persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si lo solicitan Tesorería para algún tramite extra para otro programa, siempre u cuando el ciudadano lo autorice.					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección y solo se transfiere si lo solicitan las máximas autoridades (alcalde, secretario del ayuntamiento, tesorería y auditoría del estado.					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						

<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SECRETARIA DEL AYUNTAMIENTO			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al termino de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SECRETARIA DEL AYUNTAMIENTO

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR			
<b>I.- Nombre del sistema:</b>		CONSTANCIA LABORAL	
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
<b>Administrador Responsable</b>			
<b>Nombre:</b>	Julio Cesar Molina González	<b>Cargo:</b>	Secretario del Ayuntamiento
<b>Usuario Responsable 1</b>			
<b>Nombre:</b>	Alejandra Campos Salgado	<b>Cargo:</b>	ASISTENTE
<b>Encargado</b>			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Generar una constancia donde podamos brindarle al ciudadano una recomendación para que pueda buscar trabajo		
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.		
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)		
	<b>Dato Personal</b>	<b>Idoneidad</b>	
	Nombre	Para la identificación	
	Domicilio	Para la identificación	
	Teléfono	Para la notificación en su caso	
	<b>ECONOMICOS</b> (Identificativos)		
<b>Dato Personal</b>	<b>Idoneidad</b>		
Ingreso Mensual	Para la identificación		
Ocupación	Para la identificación		
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>5 Datos</b>		
<b>Volumen de Formatos</b>	<b>15 Expedientes</b>		
<b>Cantidad Global de Datos Personales</b>	<b>75 Datos Personales Tratados</b>		
<b>Quien suministra</b>	El ciudadano del Municipio de Marín, N.L.		
<b>Cómo suministra</b>	Directamente		
<b>Forma de obtención de datos</b>	Formato		

<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para llevar control			
	<b>Documentos Adjuntos con protección de datos personales</b>		(Solo se pide copia de su ine para incluir como constancia )			
	<b>Características del lugar donde se resguardan</b>		ARCHIVERO DE OFICINA DEL SECRETARIO DEL AYUNTAMIENTO			
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b> <b>VII.- Resguardo de los Sistemas</b> <b>XII.- Medidas de seguridad aplicadas a las instalaciones</b> <b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si lo solicitan Tesorería para algún trámite extra para otro programa, siempre y cuando el ciudadano lo autorice.					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección y solo se transfiere si lo solicitan las máximas autoridades (alcalde, secretario del ayuntamiento, tesorería y auditoría del estado.					
<b>Acceso a las instalaciones</b>						

<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SECRETARIA DEL AYUNTAMIENTO			<b>Tiempo</b>	3 AÑOS	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## SECRETARIA DEL AYUNTAMIENTO

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR			
<b>I.- Nombre del sistema:</b>		PROGRAMA DE TERRENOS 3ER. SECTOR DE LA COLONIA EL SALADITO	
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>			
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
Administrador Responsable			
<b>Nombre:</b>	Julio Cesar Molina González	<b>Cargo:</b>	Secretario del Ayuntamiento
Usuario Responsable 1			
<b>Nombre:</b>	Alejandra Campos Salgado	<b>Cargo:</b>	ASISTENTE
Encargado			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b>			
<b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Generar un archivo del procedimiento de entrega del terreno,		
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L.		
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)		
	<b>Dato Personal</b>	<b>Inodeidad</b>	
	Nombre	Para la identificación	
	Domicilio	Para la identificación	
	Teléfono	Para la notificación en su caso	
	INE	Para la identificación	
	CURP	Para la identificación	
	Acta de Nacimiento	Para la identificación	
	Acta de Matrimonio	Para la identificación	
	<b>PATRIMONIALES</b> (Identificativos)		
<b>Dato Personal</b>	<b>Idoneidad</b>		
Carta de NO Propiedad	Para comprobación que no cuenta con otro predio y puedan darle el programa		
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>8 Datos</b>		
<b>Volumen de Formatos</b>	<b>122 Expedientes</b>		
<b>Cantidad Global de Datos Personales</b>	<b>976 Datos Personales Tratados</b>		
<b>Quien suministra</b>	El ciudadano del Municipio de Marín, N.L.		

<b>Cómo suministra</b>	Directamente					
<b>Forma de obtención de datos</b>	Formato, constancias,					
<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	SI
	<b>Descripción</b>		Formato establecido para llevar control			
	<b>Documentos Adjuntos con protección de datos personales</b>		INE, CURP, ACTA DE NACIMIENTO Y ACTA DE MATRIMONIO, CARTA DE NO PROPIEDAD			
<b>Características del lugar donde se resguardan</b>		ARCHIVERO DE OFICINA DEL SECRETARIO DEL AYUNTAMIENTO				
<b>Participación en el ciclo de vida del dato personal</b>	Obtención, conservación y utilización.					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico		Medio	X	Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ningún persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	Formatos llenados					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si lo solicitan Tesorería, Auditoría del Estado para su debida comprobación del programa					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	NO APLICA YA QUE NO SE ALMACENA DIGITALMENTE					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					

<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	INDEFINIDO	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA SECRETARIA DEL AYUNTAMIENTO			<b>Tiempo</b>	INDEFINIDO	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incrementa l	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						



## DESARROLLO SOCIAL

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DESARROLLO SOCIAL																						
<b>I.- Nombre del sistema:</b>		INSCRIPCIÓN AL PROGRAMA DE UNIFORMES Y ÚTILES ESCOLARES																				
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>																						
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>																						
Administrador Responsable																						
<b>Nombre:</b>	Claudia Mirna González Moreno	<b>Cargo:</b>	DIRECTORA DE DESARROLLO SOCIAL																			
Encargado																						
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA																			
<b>IV.- Inventario de datos personales</b>																						
<b>V.- Estructura y descripción de los sistemas</b>																						
<b>Objetivo:</b>	Tener el control de las personas inscritas al programa para realizar los paquetes y compras adecuadas. Apoyos a las familias de nuestro municipio con una aportación en especie para el reingreso escolar.																					
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.																					
<b>Datos Personales que se encuentran en el sistema:</b>	<p style="text-align: center;"><b>ORDINARIOS</b> (Identificativos)</p> <table border="1" style="width: 100%; border-collapse: collapse; margin: 5px 0;"> <thead> <tr> <th style="width: 50%; padding: 5px;">Dato Personal</th> <th style="width: 50%; padding: 5px;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Nombre Alumno</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Nombre del Padre</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Ocupación</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">CURP</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Fecha de Nacimiento</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Domicilio</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Teléfono</td> <td style="padding: 5px;">Para la identificación</td> </tr> </tbody> </table>						Dato Personal	Idoneidad	Nombre Alumno	Para la identificación	Nombre del Padre	Para la identificación	Ocupación	Para la identificación	CURP	Para la identificación	Fecha de Nacimiento	Para la identificación	Domicilio	Para la identificación	Teléfono	Para la identificación
Dato Personal	Idoneidad																					
Nombre Alumno	Para la identificación																					
Nombre del Padre	Para la identificación																					
Ocupación	Para la identificación																					
CURP	Para la identificación																					
Fecha de Nacimiento	Para la identificación																					
Domicilio	Para la identificación																					
Teléfono	Para la identificación																					
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>7 Datos</b>																					
<b>Volumen de Formatos</b>	<b>766 Expedientes</b>																					
<b>Cantidad Global de Datos Personales</b>	<b>5,362 Datos Personales Tratados</b>																					
<b>Quien suministra</b>	El padre, y/o niño del Municipio de Marín, N,L. que lo solicite																					
<b>Cómo suministra</b>	Directamente - Presencial																					
<b>Forma de obtención de datos</b>	Formulario																					
<b>Forma de obtención de datos</b>	Físico	SI	Electrónico	NO	Vía Telefónica	NO																

<b>Tipo de Soporte Forma de obtención de datos</b>	<b>Descripción</b>	Expediente para el apoyo				
	<b>Documentos Adjuntos con protección de datos personales</b>	INE padre/ madre de familia, curp del alumno, comprobante de domicilio				
	<b>Características del lugar donde se resguardan</b>	ARCHIVO DE OFICINA DE DESARROLLO SOCIAL OFICINA DE ARCHIVO MPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias VII.- Resguardo de los Sistemas XII.- Medidas de seguridad aplicadas a las instalaciones XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	Los Archivos se encuentran resguardados, ninguna persona ajena al departamento puede acceder.					
<b>Transferencia Físico</b>	No aplica					
<b>Medidas de seguridad transferencia física</b>	Se encuentran resguardados bajo llave en el archivero de esta área y solo se transfiere si se solicita por medio de Transparencia el ciudadano					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE cuenta bajo contraseña nadie ajeno a este departamento tiene acceso,					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						

<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE DESARROLLO SOCIAL			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIRECCIÓN DE CULTURA

UNIDAD ADMINISTRATIVA: BIBLIOTECA													
<b>I.- Nombre del sistema:</b>		PRESTAMO DE LIBROS EN BIBLIOTECA											
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>													
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>													
<b>Administrador Responsable</b>													
<b>Nombre:</b>	Guadalupe Enriqueta Hernández García	<b>Cargo:</b>	DIRECTORA										
<b>Usuario Responsable 1</b>													
<b>Nombre:</b>	Sheila Abigail González Rodríguez	<b>Cargo:</b>	Secretaria de Educación y Cultura										
<b>Encargado</b>													
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA										
<b>IV.- Inventario de datos personales</b>													
<b>V.- Estructura y descripción de los sistemas</b>													
<b>Objetivo:</b>	Tener un control de los expedientes de los usuarios que solicitan un servicio de la biblioteca, Formar parte de los requisitos para ingresar como usuario para integrar su expediente y sirva como una constancia a la persona que se le presta algún libro.												
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.												
<b>Datos Personales que se encuentran en el sistema:</b>	<p style="text-align: center;"><b>ORDINARIOS</b> (Identificativos)</p> <table border="1" style="width: 100%; border-collapse: collapse; margin: 5px 0;"> <thead> <tr> <th style="width: 50%; padding: 5px;">Dato Personal</th> <th style="width: 50%; padding: 5px;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Nombre Alumno</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Edad</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Sexo</td> <td style="padding: 5px;">Para la identificación</td> </tr> </tbody> </table>					Dato Personal	Idoneidad	Nombre Alumno	Para la identificación	Edad	Para la identificación	Sexo	Para la identificación
Dato Personal	Idoneidad												
Nombre Alumno	Para la identificación												
Edad	Para la identificación												
Sexo	Para la identificación												
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>												
<b>Volumen de Formatos</b>	<b>12 Expedientes</b>												
<b>Cantidad Global de Datos Personales</b>	<b>36 Datos Personales Tratados</b>												
<b>Quien suministra</b>	Estudiante o ciudadano del Municipio de Marín, N.L. que lo solicite												
<b>Cómo suministra</b>	Directamente - Presencial												
<b>Forma de obtención de datos</b>	Formulario												
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	NO							
<b>Descripción</b>	Expediente para el apoyo												

<b>Tipo de Soporte Forma de obtención de datos</b>						
	<b>Documentos Adjuntos con protección de datos personales</b>	SI ES MAYOR DE EDAD SE DEJA EL INE ORIGINAL, PERO SI ES MENOR DE EDAD SE DEJA UN COMPROBANTE DE DOMICILIO Y AL MOMENTO QUE SE REGRESA EL LIBRO SE LE DEVUELVE. <ul style="list-style-type: none"> <li>• INE</li> <li>• COMPROBANTE DE DOMICILIO</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVO DE OFICINA DE BIBLIOTECA OFICINA DE ARCHIVO MPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias VII.- Resguardo de los Sistemas XII.- Medidas de seguridad aplicadas a las instalaciones XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE CULTURA OCULTAS PARA INGRESAR					
<b>Transferencia Físico</b>	NO SE TRANSIERE FISICAMENTE					
<b>Medidas de seguridad transferencia física</b>	BAJO RESGUARDO					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						

<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE BIBLIOTECA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIRECCIÓN DE CULTURA

UNIDAD ADMINISTRATIVA: BIBLIOTECA																	
<b>I.- Nombre del sistema:</b>	DIVERSAS EXPRESIONES CULTURALES																
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>																	
<b>Administrador Responsable</b>																	
<b>Nombre:</b>	Guadalupe Enriqueta Hernández García	<b>Cargo:</b>	DIRECTORA														
<b>Usuario Responsable 1</b>																	
<b>Nombre:</b>	Sheila Abigail González Rodríguez	<b>Cargo:</b>	Secretaria de Educación y Cultura														
<b>Encargado</b>																	
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA														
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>																	
<b>Objetivo:</b>	Tener un control de los expedientes de los usuarios que llevan a cabo alguna actividad con expresiones culturales, representando a nuestro Municipio en festivales, exposiciones y muestras gastronómicas de cocina regional. Promover la cultura y el arte desde los diversos centros culturales, dándole continuidad a los talleres ya instalados con el apoyo de Conarte. Activar proyectos para rescatar y preservar tradiciones culturales de nuestro municipio. Realizar eventos culturales con la colaboración y coordinación del gobierno del estado y gobierno federal tales como la asociación "patrimonio". Impulsar y rescatar todas las expresiones artísticas de nuestro municipio. desarrollar un programa para conocer y reconocer a los personajes ilustres de nuestro municipio.																
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.																
<b>Datos Personales que se encuentran en el sistema:</b>	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="2" style="text-align: center;">ORDINARIOS (Identificativos)</th> </tr> <tr> <th style="width: 50%; text-align: center;">Dato Personal</th> <th style="width: 50%; text-align: center;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td>Nombre Alumno</td> <td>Para la identificación</td> </tr> <tr> <td>Edad</td> <td>Para la identificación</td> </tr> <tr> <td>Sexo</td> <td>Para la identificación</td> </tr> <tr> <td>Teléfono</td> <td>Para la identificación</td> </tr> <tr> <td>Dirección</td> <td>Para la identificación</td> </tr> </tbody> </table>			ORDINARIOS (Identificativos)		Dato Personal	Idoneidad	Nombre Alumno	Para la identificación	Edad	Para la identificación	Sexo	Para la identificación	Teléfono	Para la identificación	Dirección	Para la identificación
ORDINARIOS (Identificativos)																	
Dato Personal	Idoneidad																
Nombre Alumno	Para la identificación																
Edad	Para la identificación																
Sexo	Para la identificación																
Teléfono	Para la identificación																
Dirección	Para la identificación																
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>6 Datos</b>																

Volumen de Formatos	114 Expedientes					
Cantidad Global de Datos Personales	684 Datos Personales Tratados					
Quien suministra	Estudiante o ciudadano del Municipio de Marín, N.L. que lo solicite					
Cómo suministra	Directamente - Presencial					
Forma de obtención de datos	Formulario					
Forma de obtención de datos  Tipo de Soporte Forma de obtención de datos	Físico	SI	Electrónico	NO	Vía Telefónica	NO
	Descripción		Expediente para el apoyo			
	Documentos Adjuntos con protección de datos personales		Solo se registran en un formulario con algunos datos personales y estos se pasan a la plataforma de transparencia nacional como un padrón de beneficiarios de este servicio			
	Características del lugar donde se resguardan		ARCHIVO DE OFICINA DE BIBLIOTECA OFICINA DE ARCHIVO MPAL			
Participación en el ciclo de vida del dato personal	Obtención, conservación y utilización.					
VI.- Controles y Mecanismos de Seguridad de las transferencias VII.- Resguardo de los Sistemas XII.- Medidas de seguridad aplicadas a las instalaciones XIII.- Controles de identificación y autenticación de los usuarios						
Nivel de seguridad	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
Transferencia Electrónico y digital:	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
Medidas de seguridad transferencia electrónica digital	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE CULTURA OCULTAS PARA INGRESAR					
Transferencia Físico	NO SE TRANSFIERE FISICAMENTE					
Medidas de seguridad transferencia física	BAJO RESGUARDO					
<b>Almacenamiento Sistemas de Datos Personales</b>						
Almacenamiento Electrónico y digital:	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO
Medidas de seguridad almacenamiento electrónica digital	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					



<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE CULTURA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIRECCIÓN DE CULTURA

UNIDAD ADMINISTRATIVA: BIBLIOTECA															
<b>I.- Nombre del sistema:</b>		MODULOS DIGITALES													
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>															
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>															
<b>Administrador Responsable</b>															
<b>Nombre:</b>	Guadalupe Enriqueta Hernández García	<b>Cargo:</b>	DIRECTORA												
<b>Usuario Responsable 1</b>															
<b>Nombre:</b>	Sheila Abigail González Rodríguez	<b>Cargo:</b>	Secretaria de Educación y Cultura												
<b>Encargado</b>															
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA												
<b>IV.- Inventario de datos personales</b>															
<b>V.- Estructura y descripción de los sistemas</b>															
<b>Objetivo:</b>	Tener un control de los expedientes de los usuarios que solicitan un servicio de computación. Forma parte de los requisitos para ingresar como usuario y sirva para alguna situación con el aparato de cómputo y tener como constancia a la persona que se le presta el servicio														
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.														
<b>Datos Personales que se encuentran en el sistema:</b>	<p style="text-align: center;"><b>ORDINARIOS</b> (Identificativos)</p> <table border="1" style="width: 100%; border-collapse: collapse; margin: 5px 0;"> <thead> <tr> <th style="width: 50%; text-align: center;">Dato Personal</th> <th style="width: 50%; text-align: center;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td>Nombre Alumno</td> <td>Para la identificación</td> </tr> <tr> <td>Edad</td> <td>Para la identificación</td> </tr> <tr> <td>Sexo</td> <td>Para la identificación</td> </tr> <tr> <td>Teléfono</td> <td>Para la identificación</td> </tr> <tr> <td>Dirección</td> <td>Para la identificación</td> </tr> </tbody> </table>			Dato Personal	Idoneidad	Nombre Alumno	Para la identificación	Edad	Para la identificación	Sexo	Para la identificación	Teléfono	Para la identificación	Dirección	Para la identificación
Dato Personal	Idoneidad														
Nombre Alumno	Para la identificación														
Edad	Para la identificación														
Sexo	Para la identificación														
Teléfono	Para la identificación														
Dirección	Para la identificación														
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>6 Datos</b>														
<b>Volumen de Formatos</b>	<b>21 expedientes físico y 1251 expedientes electrónicos</b>														
<b>Cantidad Global de Datos Personales</b>	<b>7,632 Datos Personales Tratados</b>														
<b>Quien suministra</b>	Estudiante o ciudadano del Municipio de Marín, N.L. que lo solicite														
<b>Cómo suministra</b>	Directamente - Presencial														

<b>Forma de obtención de datos</b>	Formulario					
<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	NO
	<b>Descripción</b>		Expediente para el apoyo			
	<b>Documentos Adjuntos con protección de datos personales</b>		Solo se registran en un formulario con algunos datos personales y estos se pasan a la plataforma de transparencia nacional como un padrón de beneficiarios de este servicio			
	<b>Características del lugar donde se resguardan</b>		ARCHIVO DE OFICINA DE BIBLIOTECA OFICINA DE ARCHIVO MPAL			
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE CULTURA OCULTAS PARA INGRESAR					
<b>Transferencia Físico</b>	NO SE TRANSFIERE FISICAMENTE					
<b>Medidas de seguridad transferencia física</b>	BAJO RESGUARDO					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						

<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE CULTURA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIRECCIÓN DE DEPORTES

UNIDAD ADMINISTRATIVA: DIRECCION DE DEPORTES			
<b>I.- Nombre del sistema:</b>		OLIMPIADAS ESTATALES	
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>			
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
<b>Administrador Responsable</b>			
<b>Nombre:</b>	José De Jesús Benavides Guerra.	<b>Cargo:</b>	DIRECTORA
<b>Usuario Responsable 1</b>			
<b>Nombre:</b>	Claudia Nora Pacheco Alanís	<b>Cargo:</b>	ENTRENADORA DE DEPORTES
<b>Encargado</b>			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b>			
<b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Tener Un Control De Los Expedientes De Los Deportistas Que Participan En El Área De Deportes De Este Gobierno Municipal.. Formar Parte De Del Equipo Para Participar En Las Ligas Deportivas.		
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.		
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)		
	<b>Dato Personal</b>	<b>Idoneidad</b>	
	Nombre	Para la identificación	
	Dirección	Para la identificación	
	Teléfono	Para la identificación	
Datos de los Padres en caso de ser menor de edad	Para la identificación		
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>4 Datos</b>		
<b>Volumen de Formatos</b>	<b>120 expedientes</b>		
<b>Cantidad Global de Datos Personales</b>	<b>480 Datos Personales Tratados</b>		
<b>Quien suministra</b>	Estudiante o ciudadano del Municipio de Marín, N,L. que lo solicite		
<b>Cómo suministra</b>	Directamente - Presencial		
<b>Forma de obtención de datos</b>	Formato		

<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	NO
	<b>Descripción</b>		Expediente para el registro del deportista			
	<b>Documentos Adjuntos con protección de datos personales</b>		Los Datos Se Recaban De Manera Física, Ya Que Se Les requiere para comprobar en las Olimpiadas Estatales <ul style="list-style-type: none"> <li>• INE</li> <li>• CURP</li> <li>• ACTA DE NACIMIENTO</li> <li>• CARTA DE PERMISO EN CASO DE SER MENOR DE EDAD</li> </ul>			
<b>Características del lugar donde se resguardan</b>		ARCHIVO DE OFICINA DE DEPORTES OFICINA DE ARCHIVO MPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b> <b>VII.- Resguardo de los Sistemas</b> <b>XII.- Medidas de seguridad aplicadas a las instalaciones</b> <b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE DEPORTES PARA INGRESAR					
<b>Transferencia Físico</b>	NO SE TRANSFIERE FISICAMENTE AL MENOS QUE LO REQUIERA TESORERIA O AUDITORIA DEL ESTADO					
<b>Medidas de seguridad transferencia física</b>	BAJO RESGUARDO					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					

<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE DEPORTES			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia		Si		X	NO	
Se realizan pruebas de eficiencia		Si		X	NO	
Se cuenta con un sitio redundante		Si		X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIRECCIÓN DE DEPORTES

UNIDAD ADMINISTRATIVA: DIRECCION DE DEPORTES													
<b>I.- Nombre del sistema:</b>		AREA DE PESAS											
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>													
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>													
<b>Administrador Responsable</b>													
<b>Nombre:</b>	José De Jesús Benavides Guerra.	<b>Cargo:</b>	DIRECTORA										
<b>Usuario Responsable 1</b>													
<b>Nombre:</b>	Claudia Nora Pacheco Alanís	<b>Cargo:</b>	ENTRENADORA DE DEPORTES										
<b>Encargado</b>													
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA										
<b>IV.- Inventario de datos personales</b>													
<b>V.- Estructura y descripción de los sistemas</b>													
<b>Objetivo:</b>	Tener Un Control De Los Expedientes De Los Deportistas utilizan el área de pesas												
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.												
<b>Datos Personales que se encuentran en el sistema:</b>	<p style="text-align: center;"><b>ORDINARIOS</b> (Identificativos)</p> <table border="1" style="width: 100%; border-collapse: collapse; margin: 5px 0;"> <thead> <tr> <th style="width: 50%; padding: 5px;">Dato Personal</th> <th style="width: 50%; padding: 5px;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Nombre</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Dirección</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Teléfono</td> <td style="padding: 5px;">Para la identificación</td> </tr> </tbody> </table>					Dato Personal	Idoneidad	Nombre	Para la identificación	Dirección	Para la identificación	Teléfono	Para la identificación
Dato Personal	Idoneidad												
Nombre	Para la identificación												
Dirección	Para la identificación												
Teléfono	Para la identificación												
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>4 Datos</b>												
<b>Volumen de Formatos</b>	<b>220 expedientes</b>												
<b>Cantidad Global de Datos Personales</b>	<b>880 Datos Personales Tratados</b>												
<b>Quien suministra</b>	Estudiante o ciudadano del Municipio de Marín, N.L. que lo solicite												
<b>Cómo suministra</b>	Directamente - Presencial												
<b>Forma de obtención de datos</b>	Formato												
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	NO							
<b>Descripción</b>	Expediente para el registro del deportista												



<b>Tipo de Soporte Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	Los Datos Se Recaban De Manera Física, Ya Que Se Les Entrega Su Boleto De Pago. <ul style="list-style-type: none"> <li>• INE</li> <li>• CURP</li> <li>• ACTA DE NACIMIENTO</li> <li>• CARTA DE PERMISO EN CASO DE SER MENOR DE EDAD</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVO DE OFICINA DE DEPORTES OFICINA DE ARCHIVO MPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias VII.- Resguardo de los Sistemas XII.- Medidas de seguridad aplicadas a las instalaciones XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE DEPORTES PARA INGRESAR					
<b>Transferencia Físico</b>	NO SE TRANSFIERE FISICAMENTE AL MENOS QUE LO REQUIERA TESORERIA O AUDITORIA DEL ESTADO					
<b>Medidas de seguridad transferencia física</b>	BAJO RESGUARDO					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoria del Estado					
<b>Acceso a las instalaciones</b>						

<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE DEPORTES			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIRECCIÓN DE DEPORTES

UNIDAD ADMINISTRATIVA: DIRECCION DE DEPORTES													
<b>I.- Nombre del sistema:</b>		GIMNASIA											
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>													
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>													
Administrador Responsable													
<b>Nombre:</b>	José De Jesús Benavides Guerra.	<b>Cargo:</b>	DIRECTORA										
Usuario Responsable 1													
<b>Nombre:</b>	Claudia Nora Pacheco Alanís	<b>Cargo:</b>	ENTRENADORA DE DEPORTES										
Encargado													
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA										
<b>IV.- Inventario de datos personales</b>													
<b>V.- Estructura y descripción de los sistemas</b>													
<b>Objetivo:</b>	Tener Un Control De Los Expedientes De Los Deportistas												
<b>Fundamento Legal:</b>	Reglamento de la Administración Pública Municipal de Marín, N.L. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León, Título Primero, Disposiciones Generales, Capítulo I, Del Objeto De La Ley, Artículo 2, Fracción I.												
<b>Datos Personales que se encuentran en el sistema:</b>	<p style="text-align: center;"><b>ORDINARIOS</b> (Identificativos)</p> <table border="1" style="width: 100%; border-collapse: collapse; margin: 5px 0;"> <thead> <tr> <th style="width: 50%; padding: 5px;">Dato Personal</th> <th style="width: 50%; padding: 5px;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Nombre</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Dirección</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Teléfono</td> <td style="padding: 5px;">Para la identificación</td> </tr> </tbody> </table>					Dato Personal	Idoneidad	Nombre	Para la identificación	Dirección	Para la identificación	Teléfono	Para la identificación
Dato Personal	Idoneidad												
Nombre	Para la identificación												
Dirección	Para la identificación												
Teléfono	Para la identificación												
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>												
<b>Volumen de Formatos</b>	<b>60 expedientes</b>												
<b>Cantidad Global de Datos Personales</b>	<b>180 Datos Personales Tratados</b>												
<b>Quien suministra</b>	Estudiante o ciudadano del Municipio de Marín, N,L. que lo solicite												
<b>Cómo suministra</b>	Directamente - Presencial												
<b>Forma de obtención de datos</b>	Formato												
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	NO							
<b>Descripción</b>	Expediente para el registro del deportista												

<b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	<ul style="list-style-type: none"> <li>• INE DEL PADRE</li> <li>• CURP</li> <li>• ACTA DE NACIMIENTO</li> <li>• CARTA DE PERMISO EN CASO DE SER MENOR DE EDAD</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVO DE OFICINA DE DEPORTES OFICINA DE ARCHIVO MPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE DEPORTES PARA INGRESAR					
<b>Transferencia Físico</b>	NO SE TRANSFIERE FISICAMENTE AL MENOS QUE LO REQUIERA TESORERIA O AUDITORIA DEL ESTADO					
<b>Medidas de seguridad transferencia física</b>	BAJO RESGUARDO					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						

<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE DEPORTES			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIRECCIÓN DE OBRAS PÚBLICAS Y DESARROLLO URBANO

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DE OBRAS PUBLICAS Y DESARROLLO URBANO						
I.- Nombre del sistema:		ASIGNACION DE NUMEROS OFICIALES				
II.- Nombre cargo y adscripción del administrador del sistema III.- funciones y obligaciones de las personas que traten datos personales.						
<b>Administrador Responsable</b>						
Nombre:	Santiago Guadalupe Garza Nañez	Cargo:	DIRECTOR			
<b>Usuario Responsable 1</b>						
Nombre:	José Vicente Martínez Reyes	Cargo:	ADMINISTRATIVO			
<b>Encargado</b>						
Nombre:	Mayela González Gómez	Cargo:	ENLACE DE TRANSPARENCIA			
IV.- Inventario de datos personales V.- Estructura y descripción de los sistemas						
Objetivo:	Tener un control de los expedientes de las asignaciones de números oficiales. Asignar un numero oficial a los predios que no cuenten con el número.					
Fundamento Legal:	ART. 11, 315, 402 DE LA LEY DE ASENTAMIENTOS HUMANOS, ORDENAMIENTO TERRITORIAL Y DESARROLLO URBANO PARA EL ESTADO DE NUEVO LEÓN					
Datos Personales que se encuentran en el sistema:	<b>ORDINARIOS</b> (Identificativos)					
	<b>Dato Personal</b>		<b>Idoneidad</b>			
	Nombre		Para la identificación			
	Dirección		Para la identificación			
	Teléfono		Para la identificación			
Total de Datos Personales utilizados en el Sistema de Tratamiento	<b>3 Datos</b>					
Volumen de Formatos	<b>115 expedientes</b>					
Cantidad Global de Datos Personales	<b>345 Datos Personales Tratados</b>					
Quien suministra	Ciudadano del Municipio de Marín, N.L. que lo solicite					
Cómo suministra	Directamente - Presencial					
Forma de obtención de datos	Formato					
Forma de obtención de datos	Físico	SI	Electrónico	NO	Vía Telefónica	NO
	Descripción		Expediente para la asignacion			

<b>Tipo de Soporte Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>	SOLICITUD DE TRAMITE <ul style="list-style-type: none"> <li>• ESCRITURA DE PROPIEDAD</li> <li>• I.N.E.</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVO DE OFICINA OFICINA DE ARCHIVO MPAL				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias VII.- Resguardo de los Sistemas XII.- Medidas de seguridad aplicadas a las instalaciones XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE DEPORTES PARA INGRESAR					
<b>Transferencia Físico</b>	NO SE TRANSFIERE FISICAMENTE AL MENOS QUE LO REQUIERA TESORERIA O AUDITORIA DEL ESTADO					
<b>Medidas de seguridad transferencia física</b>	BAJO RESGUARDO					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						

<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE OBRAS PUBLICAS			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						



## DIRECCIÓN DE OBRAS PÚBLICAS Y DESARROLLO URBANO

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DE OBRAS PUBLICAS Y DESARROLLO URBANO															
<b>I.- Nombre del sistema:</b>		LICENCIA DE SUBDIVISION Y FUSIÓN DE PREDIOS													
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>															
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>															
Administrador Responsable															
<b>Nombre:</b>	Santiago Guadalupe Garza Nañez	<b>Cargo:</b>	DIRECTOR												
Usuario Responsable 1															
<b>Nombre:</b>	José Vicente Martínez Reyes	<b>Cargo:</b>	ADMINISTRATIVO												
Encargado															
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA												
<b>IV.- Inventario de datos personales</b>															
<b>V.- Estructura y descripción de los sistemas</b>															
<b>Objetivo:</b>	Tener un control de los expedientes de las asignaciones de subdivisiones y fusión de predios.														
<b>Fundamento Legal:</b>	ART. 11, 315, 402 DE LA LEY DE ASENTAMIENTOS HUMANOS, ORDENAMIENTO TERRITORIAL Y DESARROLLO URBANO PARA EL ESTADO DE NUEVO LEÓN														
<b>Datos Personales que se encuentran en el sistema:</b>	<p style="text-align: center;"><b>ORDINARIOS</b> (Identificativos)</p> <table border="1" style="width: 100%; border-collapse: collapse; margin: 5px 0;"> <thead> <tr> <th style="width: 50%; padding: 5px;">Dato Personal</th> <th style="width: 50%; padding: 5px;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Nombre</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Dirección</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Teléfono</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">RFC</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Fotografías del Predio</td> <td style="padding: 5px;">Para la identificación</td> </tr> </tbody> </table>			Dato Personal	Idoneidad	Nombre	Para la identificación	Dirección	Para la identificación	Teléfono	Para la identificación	RFC	Para la identificación	Fotografías del Predio	Para la identificación
Dato Personal	Idoneidad														
Nombre	Para la identificación														
Dirección	Para la identificación														
Teléfono	Para la identificación														
RFC	Para la identificación														
Fotografías del Predio	Para la identificación														
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>5 Datos</b>														
<b>Volumen de Formatos</b>	<b>20 expedientes</b>														
<b>Cantidad Global de Datos Personales</b>	<b>100 Datos Personales Tratados</b>														
<b>Quien suministra</b>	Ciudadano del Municipio de Marín, N.L. que lo solicite														
<b>Cómo suministra</b>	Directamente - Presencial														
<b>Forma de obtención de datos</b>	Formato- Soliciutd														

	Físico	SI	Electrónico	NO	Vía Telefónica	NO	
	<b>Descripción</b>		Expediente para la asignacion				
	<b>Documentos Adjuntos con protección de datos personales</b>		<b>SOLICITUD DE TRAMITE</b> <ul style="list-style-type: none"> <li>• Presentar solicitud correspondiente a trámite a realizar</li> <li>• Copia de la identificación oficial del propietario</li> <li>• copia de la identificación oficial del apoderado</li> <li>• copia del comprobante de domicilio</li> <li>• copia del contrato de compra venta o escrituras de la propiedad. en caso de persona moral copia simple de acta constitutiva.</li> <li>• copia del pago del predial actualizado</li> <li>• certificado de libertad de gravamen</li> <li>• copia de plano de localización</li> <li>• 8 copias del plano incluyendo bardas de AutoCAD</li> <li>• avalúo valor catastral</li> <li>• memorias responsivas otorgadas por el perito.</li> </ul>				
<b>Forma de obtención de datos</b>							
<b>Tipo de Soporte Forma de obtención de datos</b>							
<b>Características del lugar donde se resguardan</b>		ARCHIVO DE OFICINA OFICINA DE ARCHIVO MPAL					
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>						
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>							
<b>VII.- Resguardo de los Sistemas</b>							
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>							
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>							
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto		
<b>Transferencias de datos personales</b>							
<b>Transferencia Electrónica y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO	
	Discos externos	NO	Carpetas compartidas	NO	CD	NO	
	Correo	NO	USB	NO	Otro:	NO	
<b>Medidas de seguridad transferencia electrónica digital</b>	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE DEPORTES PARA INGRESAR						
<b>Transferencia Físico</b>	NO SE TRANSFIERE FISICAMENTE AL MENOS QUE LO REQUIERA TESORERIA O AUDITORIA DEL ESTADO						
<b>Medidas de seguridad transferencia física</b>	BAJO RESGUARDO						
<b>Almacenamiento Sistemas de Datos Personales</b>							
	Servidor	NO	Computadora	SI	Nube	NO	

<b>Almacenamiento Electrónico y digital:</b>	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE OBRAS PUBLICAS			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					

<b>Motivos:</b>	NO APLICA
<b>Plazos y condiciones para el bloqueo del sistema:</b>	
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA	
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA	
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico	

## DIRECCIÓN DE OBRAS PÚBLICAS Y DESARROLLO URBANO

<b>UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DE OBRAS PUBLICAS Y DESARROLLO URBANO</b>			
<b>I.- Nombre del sistema:</b>		LICENCIA DE USO DE SUELO, EDIFICACION Y CONSTRUCCION	
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>			
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
<b>Administrador Responsable</b>			
<b>Nombre:</b>	Santiago Guadalupe Garza Nañez	<b>Cargo:</b>	DIRECTOR
<b>Usuario Responsable 1</b>			
<b>Nombre:</b>	José Vicente Martínez Reyes	<b>Cargo:</b>	ADMINISTRATIVO
<b>Encargado</b>			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b>			
<b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Tener un control de los expedientes de las licencias de uso de suelo, edificación y construcción.Registrar y regular los usos de suelo, edificación y construcción en zonas diferentes de nuestro municipio.		
<b>Fundamento Legal:</b>	ART. 11, 315, 402 DE LA LEY DE ASENTAMIENTOS HUMANOS, ORDENAMIENTO TERRITORIAL Y DESARROLLO URBANO PARA EL ESTADO DE NUEVO LEÓN		
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)		
	<b>Dato Personal</b>	<b>Idoneidad</b>	
	Nombre	Para la identificación	
	Dirección	Para la identificación	
	Teléfono	Para la identificación	
	RFC	Para la identificación	
Fotografías del Predio	Para la identificación		
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>5 Datos</b>		

<b>Volumen de Formatos</b>	<b>17 expedientes</b>					
<b>Cantidad Global de Datos Personales</b>	<b>85 Datos Personales Tratados</b>					
<b>Quien suministra</b>	Ciudadano del Municipio de Marín, N,L. que lo solicite					
<b>Cómo suministra</b>	Directamente - Presencial					
<b>Forma de obtención de datos</b>	Formato- Solicitud					
<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	NO
	<b>Descripción</b>		Expediente para la asignación del permiso			
	<b>Documentos Adjuntos con protección de datos personales</b>		<b>SOLICITUD DE TRAMITE</b> <ul style="list-style-type: none"> <li>• Presentar solicitud correspondiente a trámite a realizar</li> <li>• Copia de la identificación oficial del propietario</li> <li>• copia de la identificación oficial del apoderado</li> <li>• copia del comprobante de domicilio</li> <li>• copia del contrato de compra venta o escrituras de la propiedad. en caso de persona moral copia simple de acta constitutiva.</li> <li>• copia del pago del predial actualizado</li> <li>• certificado de libertad de gravamen</li> <li>• copia de plano de localización</li> <li>• 8 copias del plano incluyendo bardas de AutoCAD</li> <li>• Avalúo valor catastral</li> </ul>			
	<b>Características del lugar donde se resguardan</b>		ARCHIVO DE OFICINA OFICINA DE ARCHIVO MPAL			
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE DEPORTES PARA INGRESAR					
<b>Transferencia Físico</b>	NO SE TRANSFIERE FISICAMENTE AL MENOS QUE LO REQUIERA TESORERIA O AUDITORIA DEL ESTADO					

Medidas de seguridad transferencia física	BAJO RESGUARDO					
<b>Almacenamiento Sistemas de Datos Personales</b>						
Almacenamiento Electrónico y digital:	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO
Medidas de seguridad almacenamiento electrónica digital	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					
Almacenamiento Físico	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
Medidas de seguridad almacenamiento física	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
Seguridad perimetral exterior: <b>SI SE CUENTA</b>						
Seguridad perimetral interior: <b>SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
Los datos que se registran en las bitácoras:						
Soporte de la bitácora:	Físico	SI	Electrónico	NO	Otro:	NO
Lugar de almacenamiento:	ARCHIVERO OFICINA			Tiempo	Indefinido	
Como se asegura la integridad:	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
Datos que se registran: fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
Soporte del registro:	Físico	SI	Electrónico	USB	Otro:	NO
Lugar de almacenamiento:	OFICINA DE OBRAS PUBLICAS			Tiempo	Indefinido	
Como se asegura la integridad:	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
Tipo de respaldo:	Completo	NO	Diferencial	NO	Incremental	SI
Medios para almacenar copias de seguridad	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
Procedimiento	NO APLICA					

<b>Equipo</b>	NO APLICA
<b>Personal</b>	NO APLICA
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>	
<b>Datos del sistema que será cancelado:</b> NO APLICA	
<b>Denominación:</b>	NO APLICA
<b>Motivos:</b>	NO APLICA
<b>Plazos y condiciones para el bloqueo del sistema:</b>	
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA	
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA	
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico	

## DIRECCIÓN DE SERVICIOS PÚBLICOS

<b>UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DE SERVICIOS PÚBLICOS</b>			
<b>I.- Nombre del sistema:</b>		ATENCIÓN A LA CIUDADANÍA	
<b>II.- Nombre cargo y adscripción del administrador del sistema</b>			
<b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
<b>Administrador Responsable</b>			
<b>Nombre:</b>	Raymundo López Cortez	<b>Cargo:</b>	DIRECTOR
<b>Usuario Responsable 1</b>			
<b>Nombre:</b>	Luis Alberto Medina Martínez	<b>Cargo:</b>	ADMINISTRATIVO ENCARGADO
<b>Encargado</b>			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b>			
<b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Tener un control de los expedientes de los reportes al Gobierno Municipal de Marín, N.L. Formar parte de los requisitos para integrar su expediente y sirva como evidencia ante la Auditoría Superior del Estado de Nuevo León.		
<b>Fundamento Legal:</b>	REGLAMENTO DE LA ADMINISTRACIÓN PÚBLICA MPAL		
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)		
	<b>Dato Personal</b>	<b>Idoneidad</b>	
	Nombre	Para la identificación	
	Dirección	Para la identificación	
	Teléfono	Para la identificación	
Fotografías del Predio	Para la identificación		
<b>Total de Datos Personales</b>			

utilizados en el Sistema de Tratamiento	<b>4 Datos</b>					
Volumen de Formatos	<b>2,245 expedientes</b>					
Cantidad Global de Datos Personales	<b>8,980 Datos Personales Tratados</b>					
Quien suministra	Ciudadano del Municipio de Marín, N,L. que lo solicite					
Cómo suministra	Directamente - Presencial					
Forma de obtención de datos	Formato					
<b>Forma de obtención de datos</b>  <b>Tipo de Soporte Forma de obtención de datos</b>	Físico	SI	Electrónico	NO	Vía Telefónica	NO
	Descripción		Expediente para la asignación apoyos y quejas de los ciudadanos, emergencias			
	Documentos Adjuntos con protección de datos personales		Ninguno ( solo se pide su ine para corroborar que vivan en el municipio de Marín n.l)			
Características del lugar donde se resguardan		ARCHIVO DE OFICINA OFICINA DE ARCHIVO MPAL				
<b>Participación en el ciclo de vida del dato personal</b>	Obtención, conservación y utilización.					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
Nivel de seguridad	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE DEPORTES PARA INGRESAR					
<b>Transferencia Físico</b>	NO SE TRANSFIERE FISICAMENTE AL MENOS QUE LO REQUIERA TESORERIA O AUDITORIA DEL ESTADO					
<b>Medidas de seguridad transferencia física</b>	BAJO RESGUARDO					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO



<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE SERVICIOS PUBLICOS			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						

**Procedimiento para la supresión y periodo de conservación del sistema:** NO APLICA

**Mecanismos para la supresión del sistema:** En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico

## DIRECCIÓN DE SERVICIOS PÚBLICOS

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DE SERVICIOS PÚBLICOS			
<b>I.- Nombre del sistema:</b>		RECOLECCIÓN DE RAMAS Y ESCOMBRO	
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>			
Administrador Responsable			
<b>Nombre:</b>	Raymundo López Cortez	<b>Cargo:</b>	DIRECTOR
Usuario Responsable 1			
<b>Nombre:</b>	Luis Alberto Medina Martínez	<b>Cargo:</b>	ADMINISTRATIVO ENCARGADO
Encargado			
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>			
<b>Objetivo:</b>	Tener un control de los expedientes de los reportes al Gobierno Municipal de Marín, N.L. Formar parte de los requisitos para integrar su expediente y sirva como evidencia ante la Auditoria Superior del Estado de Nuevo León.		
<b>Fundamento Legal:</b>	REGLAMENTO DE LA ADMINISTRACIÓN PUBLICA MPAL		
<b>Datos Personales que se encuentran en el sistema:</b>	<b>ORDINARIOS</b> (Identificativos)		
	<b>Dato Personal</b>	<b>Idoneidad</b>	
	Nombre	Para la identificación	
	Dirección	Para la identificación	
	Teléfono	Para la identificación	
Fotografías del Predio	Para la identificación		
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>4 Datos</b>		
<b>Volumen de Formatos</b>	<b>1,450 expedientes</b>		
<b>Cantidad Global de Datos Personales</b>	<b>5,800 Datos Personales Tratados</b>		
<b>Quien suministra</b>	Ciudadano del Municipio de Marín, N,L. que lo solicite		
<b>Cómo suministra</b>	Directamente - Presencial		

<b>Forma de obtención de datos</b>	Formato					
<b>Forma de obtención de datos</b>  <b>Tipo de Soporte</b> <b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	NO
	<b>Descripción</b>		Expediente para la asignación apoyos y quejas de los ciudadanos, emergencias (RECOLECCION DE BASURA Y ESCOMBRO) El encargado llena mediante llamada o si el ciudadano acude de manera presencial el formato físico para su solicitud.			
	<b>Documentos Adjuntos con protección de datos personales</b>		• NINGUNO (solo se pide su ine para corroborar que vivan en el municipio de Marín n.l)			
	<b>Características del lugar donde se resguardan</b>		ARCHIVO DE OFICINA OFICINA DE ARCHIVO MPAL			
<b>Participación en el ciclo de vida del dato personal</b>	Obtención, conservación y utilización.					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b> <b>VII.- Resguardo de los Sistemas</b> <b>XII.- Medidas de seguridad aplicadas a las instalaciones</b> <b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE DEPORTES PARA INGRESAR					
<b>Transferencia Físico</b>	NO SE TRANSFIERE FISICAMENTE AL MENOS QUE LO REQUIERA TESORERIA O AUDITORIA DEL ESTADO					
<b>Medidas de seguridad transferencia física</b>	BAJO RESGUARDO					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					

<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						
<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE SERVICIOS PUBLICOS			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

## DIRECCIÓN DE SEGURIDAD PÚBLICAS Y TRANSITO

UNIDAD ADMINISTRATIVA: OFICINA PARTICULAR DE SERVICIOS PÚBLICOS													
<b>I.- Nombre del sistema:</b>		CERTIFICACION PARA LICENCIAS DE CONDUCIR											
<b>II.- Nombre cargo y adscripción del administrador del sistema</b> <b>III.- funciones y obligaciones de las personas que traten datos personales.</b>													
Administrador Responsable													
<b>Nombre:</b>	Raymundo López Cortez	<b>Cargo:</b>	DIRECTOR										
Usuario Responsable 1													
<b>Nombre:</b>	Luis Alberto Medina Martínez	<b>Cargo:</b>	ADMINISTRATIVO ENCARGADO										
Encargado													
<b>Nombre:</b>	Mayela González Gómez	<b>Cargo:</b>	ENLACE DE TRANSPARENCIA										
<b>IV.- Inventario de datos personales</b> <b>V.- Estructura y descripción de los sistemas</b>													
<b>Objetivo:</b>	Certificar a los conductores que hayan pasado la prueba de conducir.												
<b>Fundamento Legal:</b>	Ley que regula la expedición de licencias para conducir del estado de Nuevo León												
<b>Datos Personales que se encuentran en el sistema:</b>	<div style="text-align: center;"><b>ORDINARIOS</b> (Identificativos)</div> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 50%; padding: 5px;">Dato Personal</th> <th style="width: 50%; padding: 5px;">Idoneidad</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Nombre</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Dirección</td> <td style="padding: 5px;">Para la identificación</td> </tr> <tr> <td style="padding: 5px;">Teléfono</td> <td style="padding: 5px;">Para la identificación</td> </tr> </tbody> </table>					Dato Personal	Idoneidad	Nombre	Para la identificación	Dirección	Para la identificación	Teléfono	Para la identificación
Dato Personal	Idoneidad												
Nombre	Para la identificación												
Dirección	Para la identificación												
Teléfono	Para la identificación												
<b>Total de Datos Personales utilizados en el Sistema de Tratamiento</b>	<b>3 Datos</b>												
<b>Volumen de Formatos</b>	<b>216 expedientes</b>												
<b>Cantidad Global de Datos Personales</b>	<b>648 Datos Personales Tratados</b>												
<b>Quien suministra</b>	Ciudadanos del Municipio de Marín, N,L. que lo solicite												
<b>Cómo suministra</b>	Directamente - Presencial												
<b>Forma de obtención de datos</b>	Formato												
<b>Forma de obtención de datos</b>	<b>Físico</b>	SI	<b>Electrónico</b>	NO	<b>Vía Telefónica</b>	NO							
<b>Tipo de Soporte</b>	<b>Descripción</b>		Expediente para la asignación de la Licencia										
<b>Forma de obtención de datos</b>	<b>Documentos Adjuntos con protección de datos personales</b>		<ul style="list-style-type: none"> <li>COPIA DE INE</li> <li>COPIA DE CURP</li> <li>COPIA DE ACTA DE NACIMIENTO</li> </ul>										

		<ul style="list-style-type: none"> <li>• COPIA DE COMPROBANTE DE DOMICILIO</li> <li>• COPIA DEL COMPROBANTE DE PAGO</li> <li>• COPIA DE SOLICITUD DE LICENCIA DE CONDUCIR</li> </ul>				
	<b>Características del lugar donde se resguardan</b>	ARCHIVO DE OFICINA OFICINA DE SEGURIDAD PÚBLICA Y VIALIDAD				
<b>Participación en el ciclo de vida del dato personal</b>	<b>Obtención, conservación y utilización.</b>					
<b>VI.- Controles y Mecanismos de Seguridad de las transferencias</b>						
<b>VII.- Resguardo de los Sistemas</b>						
<b>XII.- Medidas de seguridad aplicadas a las instalaciones</b>						
<b>XIII.- Controles de identificación y autenticación de los usuarios</b>						
<b>Nivel de seguridad</b>	Básico	X	Medio		Alto	
<b>Transferencias de datos personales</b>						
<b>Transferencia Electrónico y digital:</b>	Web service	NO	Web Transfer	NO	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	NO	USB	NO	Otro:	NO
<b>Medidas de seguridad transferencia electrónica digital</b>	SE ENCUENTRAN LAS CONTRASEÑAS DEL CORREO ELECTRONICO Y WEB TRANSFER QUE ES LA PLATAFORMA DE TRANSPARENCIA NACIONAL EN EL ÁREA DE DEPORTES PARA INGRESAR					
<b>Transferencia Físico</b>	NO SE TRANSFIERE FISICAMENTE AL MENOS QUE LO REQUIERA TESORERIA O AUDITORIA DEL ESTADO					
<b>Medidas de seguridad transferencia física</b>	BAJO RESGUARDO					
<b>Almacenamiento Sistemas de Datos Personales</b>						
<b>Almacenamiento Electrónico y digital:</b>	Servidor	NO	Computadora	SI	Nube	NO
	Discos externos	NO	Carpetas compartidas	NO	CD	NO
	Correo	SI	USB	NO	Otro:	NO
<b>Medidas de seguridad almacenamiento electrónica digital</b>	SE ENCUENTRAN CON CONTRASEÑAS DE USUARIOS DE LA COMPUTADORA PARA INGRESAR A CUALQUIER TIPO DE DATOS					
<b>Almacenamiento Físico</b>	SE ENCUENTRAN EN EL ARCHIVERO BAJO LLAVE					
<b>Medidas de seguridad almacenamiento física</b>	Se encuentran resguardados bajo llave en el archivero de esta dirección, solo para revisión de Tesorería y/o Auditoría del Estado					
<b>Acceso a las instalaciones</b>						
<b>Seguridad perimetral exterior: SI SE CUENTA</b>						
<b>Seguridad perimetral interior: SI SE CUENTA</b>						
<b>VIII.- Bitácoras para accesos y operación cotidiana</b>						

<b>Los datos que se registran en las bitácoras:</b>						
<b>Soporte de la bitácora:</b>	Físico	SI	Electrónico	NO	Otro:	NO
<b>Lugar de almacenamiento:</b>	ARCHIVERO OFICINA			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	TENER BAJO LLAVE EL ARCHIVO					
<b>XI.- Gestión de Vulneraciones</b>						
<b>Datos que se registran:</b> fecha, hora y lugar del incidente, una breve descripción del incidente que origino la vulneración, medidas adoptadas, así como nombre y firma de los involucrados.						
<b>Soporte del registro:</b>	Físico	SI	Electrónico	USB	Otro:	NO
<b>Lugar de almacenamiento:</b>	OFICINA DE POLICIA Y TRANSITO			<b>Tiempo</b>	Indefinido	
<b>Como se asegura la integridad:</b>	El respaldo durara hasta que se cuente con información nueva, generándose así uno nuevo					
<b>XIV.- Respaldo y recuperación de datos</b>						
<b>Tipo de respaldo:</b>	Completo	NO	Diferencial	NO	Incremental	SI
<b>Medios para almacenar copias de seguridad</b>	Al término de la Administración se archiva la información					
<b>XV.- Plan de Contingencia</b>						
Se cuenta con Plan de contingencia			Si	X	NO	
Se realizan pruebas de eficiencia			Si	X	NO	
Se cuenta con un sitio redundante			Si	X	NO	
<b>Procedimiento</b>	NO APLICA					
<b>Equipo</b>	NO APLICA					
<b>Personal</b>	NO APLICA					
<b>XVI.- Técnicas para la supresión y borrado seguro de los datos personales</b>						
<b>Datos del sistema que será cancelado:</b> NO APLICA						
<b>Denominación:</b>	NO APLICA					
<b>Motivos:</b>	NO APLICA					
<b>Plazos y condiciones para el bloqueo del sistema:</b>						
<b>Medidas de seguridad para el bloqueo y posterior supresión del sistema:</b> NO APLICA						
<b>Procedimiento para la supresión y periodo de conservación del sistema:</b> NO APLICA						
<b>Mecanismos para la supresión del sistema:</b> En los archivos físicos, se eliminará en el periodo de CONSERVACION según lo estipule Archivo Histórico						

# **FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES**

Para garantizar la aplicación correcta de este sistema es necesario establecer los deberes de los servidores públicos del municipio que participan en el tratamiento de los datos personales derivado de sus atribuciones, siendo estos:

## **Al momento de recibir los datos personales el servidor público que se encargue de su recepción deberá:**

- 1) Tener a la vista el Aviso de Privacidad.
- 2) Dar a conocer el aviso de privacidad al titular de los datos personales antes de la obtención de sus datos.
- 3) En caso de dudas y/o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Dirección de Transparencia.
- 4) Al obtener los datos personales cerciorarse de que la información esté completa, sea veraz y comprensible.
- 5) Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales.
- 6) 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.
- 7) Recabar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.
- 8) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.
- 9) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Marín, N.L., en el tratamiento de datos personales.
- 10) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
- 11) Tomar, cuando menos una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.
- 12) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

## **El servidor público involucrado en el tratamiento de datos personales deberá:**

- 1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Marín, N.L., en el tratamiento de datos personales.
- 2) Aplicar las medidas de seguridad correspondientes a los datos personales tratados y/o el sistema de protección en el que participa.
- 3) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.



- 4) 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 Dirección de Transparencia.
- 5) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
- 6) Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.
- 7) Tomar, cuando menos una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.
- 8) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

**El Servidor Público que administra los datos personales, conforme los sistemas de tratamiento vigentes deberán:**

- 1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Marín, N.L., en el tratamiento de datos personales.
- 2) Conocer e implementar las medidas de seguridad establecidas en el documento de seguridad.
- 3) Aplicar nuevas medidas de seguridad que resulten accesibles y viables para la protección de datos personales.
- 4) Supervisar a los servidores públicos que participan en la recepción y en el tratamiento de datos personales en cada trámite o sistema.
- 5) Tratar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.
- 6) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.
- 7) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
- 8) Tomar, cuando menos una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.
- 9) Informar a los titulares de los datos sobre nuevas finalidades del tratamiento de datos personales o nuevas transferencias.
- 10) 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 Dirección de Transparencia.
- 11) Informar a la Dirección de Transparencia 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.
- 12) Acudir a la Dirección de Transparencia en caso de asesoría sobre el tratamiento de datos personales.
- 13) Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.
- 14) Dar aviso al Comité de Transparencia, a través de la Dirección de Transparencia, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.

15) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

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

- 1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Marín, N.L., en el tratamiento de datos personales.
- 2) Implementar las medidas de seguridad que establece el documento de seguridad.
- 3) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.
- 4) Tomar una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.
- 5) 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 Dirección de Transparencia.
- 6) Aplicar medidas correctivas en caso de identificar incidentes, alteraciones o vulneraciones en el tratamiento de datos personales.
- 7) Informar a la Dirección de Transparencia 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.
- 8) Monitorear la implementación de las medidas de seguridad.
- 9) Monitorear de manera cotidiana la implementación de las medidas de seguridad y levantar actas circunstanciadas de hechos ante la reincidencia de un incumplimiento en la aplicación de las mismas.
- 10) Dar aviso al Comité de Transparencia, a través de la Dirección de Transparencia, sobre las actas circunstanciadas de hechos levantadas por el incumplimiento del documento de seguridad y sobre el seguimiento de las mismas.
- 11) Presentar propuestas de mejora o modificación del documento de seguridad a través de la Dirección de Transparencia.
- 12) Emitir reportes en relación al tratamiento de los datos personales y la aplicación de medidas de seguridad, según sea requerido por el Comité de Transparencia a través de la Dirección de Transparencia.
- 13) Diseñar, desarrollar e implementar políticas públicas, procesos internos, y/o sistemas o plataformas tecnológicas necesarias para el ejercicio de sus funciones apegándose en todo momento al documento de seguridad, las políticas o lineamientos que para el tratamiento de datos personales emita el Comité de Transparencia, la Dirección de Transparencia y el Instituto de Transparencia del Estado de Nuevo León, así como a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.
- 14) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León.

**Son obligaciones del Comité de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 87 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León:**

- 1) Revisar anualmente las políticas y/o lineamientos en materia de protección de datos personales establecidos en el presente documento.
- 2) Emitir o aprobar anualmente un programa de capacitaciones en materia de protección de datos personales.
- 3) Requerir anualmente a las dependencias o áreas responsables que tratan datos personales a través de la Dirección de Transparencia, informes sobre el tratamiento de los datos personales y la aplicación de medidas de seguridad, así como vulneraciones detectadas en el año.

**Son obligaciones de la Dirección de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 88 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León:**

- 1) Difundir al interior del Gobierno Municipal de Marín, N.L. el aviso de privacidad y el documento de seguridad.
- 2) Revisión física anual a 5 dependencias sobre el tratamiento de datos personales y la implementación de medidas de seguridad.
- 3) Proponer al Comité de Transparencia actualizaciones o modificaciones al documento de seguridad.
- 4) Emitir un reporte anual al Comité de Transparencia sobre el ejercicio de estas funciones.

El Órgano Interno de Control, conforme a sus atribuciones establecidas en el Reglamento Interior de la Administración Pública Municipal de Marín, N.L., podrá hacer revisiones o auditorías sobre la aplicación del presente documento de seguridad.

## **MEDIDAS DE SEGURIDAD**

En el presente apartado se integra la información de las medidas de seguridad de los sistemas de tratamiento de datos personales, conforme a los siguientes conceptos:

- a). Análisis de riesgos,
- b). Análisis de brecha y
- c). Plan de trabajo.

La normatividad establece que se entenderá como medidas de seguridad al conjunto de acciones, actividades, controles o mecanismos administrativos, físicos y técnicos que permiten proteger los datos personales.

El artículo 36 de la Ley estatal dispone que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confiabilidad, integridad y disponibilidad.

En tanto que el artículo 38 prevé que, para establecer y mantener las medidas de seguridad para la protección de datos personales, el responsable deberá realizar las siguientes actividades:

- Crear políticas internas para la gestión y tratamiento de los datos personales que consideren su obtención, uso y posterior supresión.
- Definir funciones y obligaciones del personal involucrado en el tratamiento de datos personales.
- Elaborar un inventario de los datos personales y de los sistemas de tratamiento.
- Realizar un análisis de riesgo de los datos personales.
- Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.
- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas de cumplimiento de las políticas de gestión y tratamiento de datos personales.
- Monitorear las medidas de seguridad implementadas, así como las amenazas y vulneraciones.
- Diseñar y aplicar distintos niveles de capacitación de personal, dependiendo de sus roles y responsabilidades en el tratamiento de datos personales.

**Medidas de seguridad:** Se abordan de tres modalidades: administrativas, físicas y técnicas.

**Las medidas de seguridad administrativas** se traducen en políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación clasificación y borrado seguro de la información; así como la sensibilización y capacitación del personal en materia de protección de datos personales.

**Las Medidas de seguridad físicas.** Son el 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 el hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

En tal sentido y de manera general en el Municipio de Marín, Nuevo León, se cuenta con las medidas de seguridad siguientes:

- **De tipo Administrativo.** Recién se han elaborado políticas internas para la gestión y tratamiento de los datos personales.

- **De tipo físico.** La Dirección de Protección Civil de la Secretaría del Republicano Ayuntamiento salvaguardan la integridad y seguridad de las personas, bienes,

activos e instalaciones del Municipio de Marín, Nuevo León, mediante procedimientos y mecanismos institucionales de identificación y prevención de riesgos de seguridad, como:

- a) Prevenir el acceso no autorizado al perímetro de organización de las dependencias, sus instalaciones físicas, áreas críticas, recursos e información: mediante control de accesos, de recepción, vigilancia, control de estacionamientos.
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas, recursos e información, contando con procedimientos y medidas de seguridad integradas en el programa de protección civil: protocolos de acceso a las áreas estratégicas, ante manifestaciones, amenazas de bomba, sismos y de incendio.
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que puedan salir de las oficinas. Se cuenta con acciones y mecanismos que permiten proteger e identificar los equipos móviles y portátiles; mobiliario, documentos y materiales mediante controles tales como pases de salida autorizado por el director del área.
- d) Proveer a los equipos de un mantenimiento eficaz, que asegure su disponibilidad e integridad. Los equipos de cómputo de escritorio y portátiles que se asignan a los servidores públicos y dependencias para el cumplimiento de sus funciones, así como los destinados al procesamiento, almacenamiento, transmisión y respaldo de la información relacionada a los sistemas de información institucionales, cuentan con un mantenimiento periódico con acciones preventivas y en su caso correctivas realizadas con personal especializado o por el fabricante, con lo que se promueve un mantenimiento eficaz, disponibilidad de equipos y la información hospedada.

- **De tipo Técnico:** Son las que se consideran aplicables para los sistemas de tratamiento de datos en soporte electrónico (Hardware y Software) Para prevenir que el acceso a las bases de datos o a la información y a los recursos, sea realizado solo por usuarios identificados y autorizados.

El acceso a las bases de datos de cada unidad administrativa es exclusivo para personal de su adscripción, incluido el personal que da soporte, y aquellos autorizados.

- a) El acceso se efectúa a través de segmentos de red.
- b) Para generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones. Las funciones del usuario de los sistemas de información institucionales son definidas por las áreas responsables de los procesos correspondientes, así como de validar su perfil.
- c) Para revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del hardware y software.
- d) Para gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos. Mediante revisión de sistemas de información, que identifiquen aquellos que estén fuera de servicio.

Los sistemas de información operan desde centros de datos resguardados físicamente. El centro de datos cuenta con un sistema de control de incendios,

control de acceso físico, respaldo de suministro eléctrico, monitoreos constantemente, complementado con inspección física diaria.

En general la seguridad lógica de los sistemas de información es resguardada a través de dichas medidas que son generales por lo que no se abordan en el análisis específico de cada uno de los sistemas.

En el caso de sistemas que sean administrados por un Encargado, se atiende a las medidas de seguridad establecidas en el instrumento jurídico que se haya formalizado.

## a) Análisis de riesgos

En el establecimiento de las medidas de seguridad, se debe considerar los riesgos existentes y la posibilidad de mitigarlos a través de un análisis cualitativo, sobre el impacto y la probabilidad de que una amenaza vulnere la seguridad, tanto en la información de los datos personales como en los recursos involucrados. Para realizar el análisis se tomó en cuenta la metodología planteada por INFO NL, que considera evaluar cuantitativa y cualitativamente sobre la posibilidad de que un activo de información pueda sufrir pérdida o daño, por lo que hay que realizar una clasificación de los datos personales para ponderar el riesgo e identificar la información, que por orden de prioridad requiere más protección.

Para poder dar valor a los niveles de riesgo se realiza una ponderación en base al **Valor de la gravedad y la Probabilidad** de que ocurran.

Para determinar el valor de gravedad se considera dos variables: el volumen de datos personales y su sensibilidad; mientras que para establecer la probabilidad de que ocurra se considera el nivel de exposición y su trazabilidad.

El análisis de riesgo se basa en tablas; así como la matriz de análisis. Por otra parte, para poder cuantificar el nivel de riesgo se utiliza la ecuación algebraica siguiente:  $(a+b)*(c+d)$ , la que se puede interpretar como la sumatoria entre: **volumen** de los datos más, **sensibilidad de los mismos**. Donde el **producto** obtenido se multiplica por el resultado de la suma entre **Nivel de exposición** más **trazabilidad**.

Al respecto se solicitó a todas las unidades administrativas de las secretarías y direcciones, la aplicación de dicha metodología en cada sistema o base de datos; resultando la siguiente matriz:

MATRIZ DE ANALISIS DE RIESGOS									
IDENTIFICACIÓN			ANÁLISIS				EVALUACIÓN		
Activo	Riesgo	vulnerabilidad	Gravedad		Probabilidad		Calificación	Nivel riesgo	
			V	S	NE	T			
Hardware	Falla en el equipo de computo	Mantenimiento insuficiente	3	2	2	1	15	Medio	
	Equipos de cómputo dañados	Falta de presupuesto para sustituir equipos	3	2	2	1	15	Medio	
	Polvo, corrosión, congelamiento, fuego, agua, contaminación radiación electromagnética	Aparatos electrónicos susceptibles a daño físico	3	2	2	1	15	Medio	
	Falla en el funcionamiento del equipo	Falta de configuraciones adecuadas	3	2	2	1	15	Medio	
	Pérdida de suministro eléctrico	Susceptibilidad a los cambios de voltaje	3	2	2	1	15	Medio	
	Fenómenos meteorológicos	Susceptibilidad a las variaciones del ambiente	3	2	2	1	15	Medio	
	Robo de información electrónica	Almacenamiento no cifrado	3	2	2	1	15	Medio	
	Robo de información y/o soportes electrónicos	Falta de cuidado en la destrucción de soportes electrónicos	3	2	2	1	15	Medio	
	Software	Error en la operación de la aplicación	Carencia o falta de pruebas al software y su configuración	3	2	2	1	15	Medio
		Abuso de derechos por parte de los usuarios	Falta de actualizaciones de seguridad en software	3	2	2	1	15	Medio
Acceso no autorizado a los sistemas		No cerrar la sesión al abandonar la estación de trabajo	3	2	2	1	15	Medio	
Consulta de información confidencial		Desecho o reutilización de medios de almacenamiento sin un adecuado borrado de información	3	2	2	1	15	Medio	
Acciones fraudulentas		Falta de registros de auditoría	3	2	2	1	15	Medio	
Intrusión en los sistemas		Error en las asignaciones de derechos de acceso	3	2	2	1	15	Medio	
Datos incorrectos		Copiado incontrolado de información	3	2	2	1	15	Medio	
Error en la operación de los sistemas		Interfases de usuario complicadas	3	2	2	1	15	Medio	
		Suplantación de identidad	Falla de mecanismos de identificación y autenticación de usuario	3	2	2	1	15	Medio
		Penetración y manipulación de los sistemas	Contraseñas no cifradas	3	2	2	1	15	Medio

Redes	Hacker, craker	Acceso no autorizado al sistema	3	2	2	1	15	Medio
	Hacker, craker	Robo de información	3	2	2	1	15	Medio
	Intrusión a la privacidad de los servidores públicos municipales	Servicios de red habilitados innecesarios	3	2	2	1	15	Medio
	Ejecución de código malicioso	Descarga y uso de software no controlado	3	2	2	1	15	Medio
	Corrupción de datos en los sistemas	Falta de respaldos	3	2	2	1	15	Medio
	Uso no autorizado de los servicios	Falta de un registro sobre la administración de los recursos	3	2	2	1	15	Medio
	Espionaje o escucha de comunicaciones	Lineas de comunicación sin protección	3	2	2	1	15	Medio
	Mal funcionamiento en los equipos de telecomunicaciones	Cableado de interconexión dañado o antiguo	3	2	2	1	15	Medio
Personal Municipal	Espionaje o escucha de comunicaciones	Arquitectura de red insegura	3	2	2	1	15	Medio
	Fraude y robo	Falta de personal sensibilizado y/o entrenado en seguridad	3	2	2	1	15	Medio
	Fraude y robo	Proceso de reclutamiento inadecuado	3	2	2	1	15	Medio
	Error en las operaciones de los sistemas	Uso incorrecto de software y hardware	3	2	2	1	15	Medio
	Robo de información y/o soportes físicos/electrónicos	Falta de supervisión al trabajo de externos	3	2	2	1	15	Medio
	Negligencia laboral	Errores de captura de información	3	2	2	1	15	Medio
	Uso de equipo no autorizado	Falta de políticas acerca del uso de medios de telecomunicaciones	3	2	2	1	15	Medio
	Sites	Robo o destrucción de activos	Falta o implementación inadecuada de controles de acceso	3	2	2	1	15
inundaciones		Lugar susceptible al daño por agua	3	2	2	1	15	Medio
Variación de voltaje		Red eléctrica inestable	3	2	2	1	15	Medio
Institucional	Abuso de derechos por parte de los ciudadanos	Falta de asignación de responsabilidades respecto a la seguridad de la información	3	2	2	1	15	Medio
	Abuso de derechos por parte de los usuarios	Falta de registros de actividad/ bitácoras en los sistemas de administración u operación	3	2	2	1	15	Medio
	Abuso de derechos por parte de los empleados	Falta de procedimientos formales para la administración de derechos de los usuarios	3	2	2	1	15	Medio
	Abuso de derechos por parte de encargados	Falta o insuficiencia de previsiones en la realización de contratos con terceros	3	2	2	1	15	Medio
	Riesgos no identificados	Falla o ausencia de reportes de fallas	3	2	2	1	15	Medio



	Mal funcionamiento de las políticas en materia de datos personales	Falta de procedimiento formal para documentar y supervisar dichas políticas	3	2	2	1	15	Medio
	Abuso de derechos por parte de los usuarios	Falta de asignación de responsabilidades respecto a la seguridad de la información	3	2	2	1	15	Medio
	Fuga de información	Falta de políticas de sanciones administrativas y el uso de correo electrónico institucional	3	2	2	1	15	Medio
	Fallas en los sistemas de información	Faltas de procedimientos para la instalación y actualización de los sistemas de información	3	2	2	1	15	Medio
	Equipo activo y pasivo para redes	Espacio para el personal de Informática y Sistemas municipal	3	2	2	1	15	Medio
	Incumplimiento a la LPDPPSO NL	Falta de procesos para el tratamiento de datos personales	3	2	2	1	15	Medio
	Empleado negligente	Falta o insuficiencia de condiciones relacionadas a la protección de datos en contratos con empleados	3	2	2	1	15	Medio
	Mal funcionamiento de las medidas de seguridad implementadas	Falta de procesos estrictos en caso de un incidente o vulneración de seguridad	3	2	2	1	15	Medio
	Robo de datos personales	Falta de política para el uso de activos fuera de la organización	3	2	2	1	15	Medio
	Acceso no autorizado a los sistemas	Falta o insuficiencia de políticas de "escritorio limpio"	3	2	2	1	15	Medio
	Falta de mejora de las políticas en materia de PDP	Falta de mecanismos de monitoreo para vulneraciones a la seguridad de los datos	3	2	2	1	15	Medio
	Código malicioso	Falta de procedimientos para reportar puntos débiles en la seguridad	3	2	2	1	15	Medio

## b) Análisis de brecha

En relación a la evaluación general de las medidas de seguridad para minimizar la ocurrencia y el impacto de las vulneraciones a la seguridad de los datos personales, se aplicó el cuestionario del **evaluador de vulneraciones 1.0** del INAI, el cual comprende 105 preguntas clasificadas en función al **ciclo de datos personales - tipo tratamiento- y dominio -R, U, C, A y D-**, siendo los siguientes:

## **Recolección**

R.1 Herramientas automatizadas y **plataformas en línea** donde se recaban DP.

R.2 · Gestión de datos personales que no son necesarios para el tratamiento

R.3 · Recepción de transferencias o remisiones de datos personales

R.4 · Recolección de datos personales a través de un encargado o tercero

## **Uso o aprovechamiento**

U.1 · Gestión del uso o aprovechamiento de datos personales

U.2 · Autenticación de los usuarios en los sistemas de tratamiento de DP

U.3 · Control de acceso a los sistemas de tratamiento de datos personales

U.4 · Auditorías a los sistemas de tratamiento de datos personales

U.5 · Gestión de documentos físicos

U.6 · Desarrollo de aplicaciones o software que utilice datos personales

U.7 · Aplicación de procesos de anonimización, minimización y generalización para el uso de datos personales

## **Comunicación**

C.1 · Control de comunicaciones internas de datos personales

C.2 · Gestión de transferencias, remisiones y revelaciones de datos personales

C.3 · Aplicación de procesos de anonimización, minimización y generalización para transferencias y remisiones

C.4 · Seguridad durante transferencias y remisiones de datos personales

## **Almacenamiento**

A.1 · Gestión de almacenamiento de DP soportes físicos y electrónicos

A.2 · Gestión de medios extraíbles de almacenamiento electrónico

A.3 · RespalDOS de datos personales

A.4 · Respuesta a incidentes de seguridad en los sistemas de tratamiento de DP

## **Destrucción o Eliminación**

D.1 · Borrado seguro de datos personales

De lo anterior, se pudo identificar que se tiene un sistema de gestión en proceso y que para los sistemas de información de manera general se cuenta con muchas de las medidas de seguridad recomendadas, conforme a lo siguiente:

El Municipio de Marín, N.L. ha implementado un sistema de protección perimetral que ayuda a cuidar toda la información que maneja el municipio contra ataques de hackeo. Se han establecido cercos digitales de protección a las bases de datos, con un rastreo de los movimientos que se generan a las mismas en varias instancias de monitoreo.

Por otro lado, se cuenta con servicios de protección digital para las computadoras de los colaboradores y para aquellos que trabajan desde casa lo tienen que hacer mediante un VPN encriptada para cuidar la integridad de la información.

## **c) Plan de Trabajo**

La existencia del documento de seguridad, busca enmarcar los deberes del Gobierno Municipal de Marín, N.L., para la máxima protección de datos personales, ello 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 es plasmar de manera enunciativa, más no limitativa, las actividades que el Gobierno Municipal de Marín, N.L., realizará para la aplicación del presente documento de seguridad, lo anterior se realizará en base a las atribuciones establecidas en el la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Nuevo León.

Para la ejecución del presente documento de seguridad, dentro de los 6 meses siguientes a la emisión del presente documento:

- 1) Se emitirá circular para difundir la emisión del presente documento, a través de la cual se remitirá copia digital del mismo a todos los correos institucionales vigentes.
- 2) Se comunicará a los enlaces sobre la emisión del documento de seguridad, solicitando su apoyo para la difusión interna del mismo.
- 3) Se buscará una primera capacitación básica para los servidores públicos que recaban datos personales.

El Comité de Transparencia revisará cada 6 meses, a partir de la emisión del presente documento de seguridad:

- 1) Revisar lo concerniente al índice de Datos Personales y mantenerlo actualizado.
- 2) Actualizar las medidas de Seguridad conforme al Sistema de Protección de Datos Personales hecho para el Gobierno Municipal de Marín, N.L.
- 3) Actualizar el presente plan de trabajo.
- 4) Se emitirá un programa anual de capacitaciones y además se promoverá que el personal del Gobierno Municipal de Marín, N.L. se mantenga capacitado no sólo por sus áreas internas, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

## **PLAN DE CONTINGENCIA**

Ante la pérdida total o parcial de datos personales en posesión de este sujeto obligado, se debe contar con un plan de contingencia.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones a las que nos encontramos expuestos, nos encontramos con que el plan de contingencias de este sujeto obligado consiste en la aplicación de las medidas de seguridad tratadas en el apartado anterior, mismas que están sujetas a cambios por eventualidades no contempladas, por ello la importancia de señalar que el presente se trata de un plan de contingencia no limitativo.

Lo anterior toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, y al igual existan riesgos inminentes que día a día evoluciona. Con la aplicación de las medidas de seguridad establecidas en este documento se buscan minimizar los riesgos o vulneraciones, pero a su vez se intenta propiciar el restablecimiento de los datos personales en el menor tiempo posible ante cualquier eventualidad.

## **MECANISMOS DE MONITOREO**

Conforme a lo dispuesto en la Ley estatal en la materia, el responsable deberá establecer mecanismos para monitorear y revisar periódicamente las medidas de seguridad que se implementen, así como las amenazas y vulneraciones que puedan tener los datos personales. Lo anterior en base a un programa de trabajo propuesto por las unidades administrativas de cada dependencia o entidad, requiriéndose al administrador de cada sistema de tratamiento de datos personales evidencia de las acciones que se realicen.

Una vez implementadas las medidas que se propongan por las dependencias o entidades que tratan datos personales, se estará en posibilidad de elaborarse un programa para revisar la eficiencia y eficacia del sistema general de gestión de la seguridad de datos personales.

En caso de existir la figura de encargado se deberán revisar los instrumentos jurídicos en cuanto a las medidas de seguridad y mecanismos de monitoreo que se hayan considerado. Se solicitará a las áreas administrativas de las secretarías y direcciones, dichos documentos para verificar si están incorporadas las medidas referidas y en su caso su vigencia.

## **PROGRAMA GENERAL DE CAPACITACIÓN**

La coordinación de la capacitación en el tema, corresponde a la Unidad de Transparencia bajo la tutela del Comité de Transparencia; el cual entre sus atribuciones en la materia de protección de datos personales, tiene la de establecer programas de capacitación y actualización para los servidores públicos, de conformidad a los artículos 57 fracción VI y 98 fracción VII de las leyes de Transparencia y Acceso a la Información Pública y la de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Nuevo León respectivamente.

En tal sentido se tiene la propuesta de capacitación, una genérica respecto a la protección de datos personales y una específica respecto a cada sistema de tratamiento de datos personales para el año 2021, a los involucrados considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y del perfil de puestos.

Se prevé impartir la primera capacitación general en el mes de Enero de cada año principalmente para los administradores y los operadores de los mismos, así como de los enlaces de datos personales de cada dependencia o entidad. Cabe aclarar que actualmente está pendiente la designación de dicha figura.

La capacitación abordará los siguientes temas:

- Teoría y normatividad en materia de Datos Personales
- Principios, deberes y derechos
- Responsabilidades de los operadores

- Medidas de seguridad a observar
- Medidas de apremio y sanciones

Respecto al programa específico, para cada secretaría y dirección se abordarán las temáticas con problemática en los sistemas de tratamiento bajo su responsabilidad.

## **ACTUALIZACIONES**

Conforme al artículo 42 de la ley estatal de la materia, el presente documento de seguridad deberá ser actualizado por la ocurrencia de alguno de los siguientes eventos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
- Por la Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Así también, la actualización general procederá cuando se establezca un nuevo sistema de tratamiento de datos personales o por la creación de bases de datos personales, independientemente del soporte; así como, por la emisión de herramientas metodológicas por parte de los órganos garantes, debiendo informar a la Unidad de Transparencia para su integración al inventario determinado en el presente documento.

En caso de ser actualizado, deberá nuevamente ser aprobado por el comité de Transparencia.

### **APROBACIÓN DEL DOCUMENTO DE SEGURIDAD**

**Se aprueba el presente DOCUMENTO DE SEGURIDAD DEL MUNICIPIO DE MARÍN, NUEVO LEÓN, por los integrantes del Comité de Transparencia municipal, en Marín, Nuevo León, el día \_\_\_\_\_ del año 2024 -dos mil veinticuatro-.**