DOCUMENTO DE SEGURIDAD

El presente documento contiene, describe y da cuenta de las medidas de seguridad técnicas, físicas y administrativas adoptadas por el ***Sistema para el Desarrollo Integral de la Familia del Municipio de Zapopan, Jalisco***, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

2021

I. Introducción

Mediante la promulgación del **Decreto 26420/LXI/17** el Congreso del Estado de Jalisco expidió la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios;* cuerpo normativo que establece las bases, principios, procedimientos y tratamiento que permite garantizar la protección de datos personales de los ciudadanos en posesión de los sujetos obligados responsables;

Ahora bien, en específico, los artículos 3.1 fracción XIV, y del 30 al 44 de dicho ordenamiento legal imponen la obligación de elaborar y aprobar un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo conforme a la normatividad de la materia.

Teniendo como base dicha normatividad, y tomando en consideración lo establecido en la "***Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales del 2015***[1]", emitida por el entonces Instituto Federal de Acceso a la, Información, y la "***Guía para Elaborar un Documento de Seguridad***[2]" aprobada por el Pleno del **Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco,** en la Vigésima Octava Sesión Ordinaria, celebra el 22 veintidós de agosto del año 2018 dos mil dieciocho, se crea el presente **DOCUMENTO DE SEGURIDAD**.

[1] La cual puede ser consultada en la siguiente liga electrónica: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

[2] La cual puede ser consultada en la siguiente liga electrónica: http://www.itei.org.mx/v3/documentos/guias/guia_documento_seguridad_so_31082018.pdf

CATÁLOGO DE SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de la Dirección de Servicios
Respecto del administrador de éste	**Nombre**	Lic. Guillermo Loza Garcilita
	Cargo	Director de servicios
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, fecha y lugar de nacimiento, edad, sexo, nacionalidad, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Única de Registro de Población, RFC, número credencial de elector u otra identificación, estado civil, fotografía, parentescos, familiares o dependientes económicos. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento; Secretarias del departamento; y Auxiliares Administrativos;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	21 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento del Centro Metropolitano del Adulto Mayor
Respecto del administrador de éste	**Nombre**	María Guadalupe Díaz González
	Cargo	Jefa del Departamento del Centro Metropolitano del Adulto Mayor
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, fecha y lugar de nacimiento, edad, sexo, nacionalidad, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Única de Registro de Población, RFC, número credencial de elector u otra identificación, estado civil, fotografía, parentescos, familiares o dependientes económicos. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento del Centro Metropolitano del Adulto Mayor; Secretarias del departamento; Auxiliares Administrativos; Trabajadores Sociales; Abogados del Departamento; Psicólogo del Departamento; Enfermera del Departamento; Odontólogas del Departamento; y Podólogo del Departamento.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de Autismo
Respecto del administrador de éste	**Nombre**	Lic. Carlos Eduardo Núñez Contreras
	Cargo	Jefe del Departamento de Autismo
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, fecha y lugar de nacimiento, edad, sexo, nacionalidad, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Única de Registro de Población, RFC, número credencial de elector u otra identificación, estado civil, fotografía, parentescos, familiares o dependientes económicos. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual tiene acceso el responsable del Departamento y el personal a su cargo.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.

El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitácora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento de Autismo; Auxiliares o secretarias del departamento; Educadoras del Departamento; Psicólogas del departamento ; Coordinadora de Autismo.
Procedimientos de respaldo y recuperación de datos personales	Se tiene resguardado el padrón de usuarios en el disco duro de la computadora y copia en USB, mientras que el expediente del usuario únicamente se encuentra en físico.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia

Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento no se cuenta con programa para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de Salud y Bienestar
Respecto del administrador de éste	**Nombre**	Dra. Socorro María Guadalupe Pastrana Pérez
	Cargo	Coordinadora de Salud y Bienestar
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, fecha y lugar de nacimiento, edad, sexo, nacionalidad, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Única de Registro de Población, RFC, número credencial de elector u otra identificación, estado civil, fotografía, parentescos, familiares o dependientes económicos. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.**

Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con

	otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento de Salud y Bienestar; Médico general del departamento ; Trabajadoras Social del departamento ; Auxiliar Administrativo del departamento ; Secretarias del Departamento.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene la información en el Disco Duro de la computadora.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Autismo
Respecto del administrador de éste	**Nombre**	Lic. Ruth Araceli Reyes Melchor
	Cargo	Coordinadora de Autismo
	Adscripción	Departamento de Autismo

Las funciones y obligaciones de las personas que traten datos personales	•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales	DATOS PERSONALES.- Nombre, fecha y lugar de nacimiento, edad, sexo, nacionalidad, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Única de Registro de Población, RFC, número credencial de elector u otra identificación, estado civil, fotografía, parentescos, familiares o dependientes económicos. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos digitales, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable de la Coordinación
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos

Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Coordinador de Autismo; Jefe de Departamento de Autismo; y Auxiliares o secretarias del departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia en PDF del expediente.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Al momento no se cuenta con programa para la supresión y borrado seguro de los datos personales

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad	Verificación por parte del encargado de Protección de Datos Personales de DIF Zapopan, para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento	
Programa General de capacitación		
Fecha	**Tipo de capacitación**	**Tipo de personal**

Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de Habilidades y profesionalización
Respecto del administrador de éste	**Nombre**	Lic. María Eugenia Sánchez Yarce
	Cargo	Jefa del Departamento de Habilidades y Profesionalización
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, correo electrónico particular, Clave Única de Registro de Población, fecha y lugar de nacimiento. **DATOS PERSONALES SENSIBLES.- Parentescos, Fotografía, Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos y preferencia sexual.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.

Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento; Secretarias del departamento; Auxiliares Administrativos;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	21 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Lic. Ma. Margarita Torres Vargas
	Cargo	Jefa de Área
	Adscripción	Centros de Atención
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y emocional e historial médico.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en un archivero con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.

Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, con llave.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas de los Centros de Atención, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.

Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Área, Trabajadora Social del departamento, Psicóloga del departamento, Médico General del departamento, Auxiliares administrativos o secretarias del departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Lic. Natalia Eugenia Ruelas Mejía
	Cargo	Jefa de Área
	Adscripción	Centros de Atención

Las funciones y obligaciones de las personas que traten datos personales	•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales	DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y emocional e historial médico.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos físicos en un archivero con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero de madera, con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen iesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o lestrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, lteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas le seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas le seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de espaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, con llave.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta metálica con cristal y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas de los Centros de Atención, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archiveros de madera con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Área, Trabajadora Social del departamento, Psicóloga del departamento, Médico General del departamento, Auxiliares administrativos o secretarias del departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Lic. Irma Espinoza Estrada
	Cargo	Jefa de Área
	Adscripción	Centros de Atención
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y emocional e historial médico.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en un archivero con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos

Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, con llave.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas de los Centros de Atención, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Área, Trabajadora Social del departamento, Psicóloga del departamento, Médico General del departamento, Auxiliares administrativos o secretarias del departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad	Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación		
Fecha	**Tipo de capacitación**	**Tipo de personal**

Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de octubre de 2021.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Lic. María de Carmen Karina Soria Hernández
	Cargo	Jefa de Área
	Adscripción	Centros de Atención
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y emocional e historial médico.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en un archivero con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.

Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, con llave.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas de los Centros de Atención, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Área, Trabajadora Social del departamento, Psicóloga del departamento, Médico General del departamento, Auxiliares administrativos o secretarias del departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de octubre de 2021.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Lic. Ruth Verónica Sánchez Solano
	Cargo	Jefa de Área
	Adscripción	Centros de Atención
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y emocional e historial médico.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en un archivero con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.

Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, con llave.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta con chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas de los Centros de Atención, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Área, Trabajadora Social del departamento, Psicóloga del departamento, Médico General del departamento,

	Auxiliares administrativos o secretarias del departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Lic. Natalia E. Ruelas Mejía
	Cargo	Jefa de Área
	Adscripción	Centros de Atención
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

Inventario de los datos personales	DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y emocional e historial médico.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos físicos en un archivero con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, con llave.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta con chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas de los Centros de Atención, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Área, Trabajadora Social del departamento, Psicóloga del departamento, Médico General del departamento, Auxiliares administrativos o secretarias del departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Lic. Mónica Gómez Meza
	Cargo	Jefa de Área
	Adscripción	Centros de Atención

Las funciones y obligaciones de las personas que traten datos personales	•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales	DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y emocional e historial médico.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos físicos en un archivero con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero de madera, con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, con llave.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta metálica con chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas de los Centros de Atención, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Área, Trabajadora Social del departamento, Psicóloga del departamento, Médico General del departamento, Auxiliares administrativos o secretarias del departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Lic. Denise Margarita Chávez Sánchez
	Cargo	Jefa de Área
	Adscripción	Centros de Atención
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y emocional e historial médico.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en un archivero con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos

Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, con llave.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta con chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas de los Centros de Atención, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Área, Trabajadora Social del departamento, Psicóloga del departamento, Médico General del departamento, Auxiliares administrativos o secretarias del departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad	Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación		
Fecha	**Tipo de capacitación**	**Tipo de personal**

Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Lic. Myriam Heidy Rodríguez Salcido
	Cargo	Jefa de Área
	Adscripción	Centros de Atención
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y emocional e historial médico.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en un archivero con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.

Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, con llave.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta con chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas de los Centros de Atención, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Área, Trabajadora Social del departamento, Psicóloga del departamento, Médico General del departamento, Auxiliares administrativos o secretarias del departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	
	Cargo	Jefa de Área
	Adscripción	Centros de Atención
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y emocional e historial médico.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en un archivero con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.

Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, con llave.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta con chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas de los Centros de Atención, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Área, Trabajadora Social del departamento, Psicóloga del departamento, Médico General del departamento, Auxiliares administrativos o secretarias del departamento

Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de Trabajo Social
Respecto del administrador de éste	**Nombre**	Lic. Yadira Noemí Pérez Villa
	Cargo	Jefa del Departamento de Trabajo Social
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

Inventario de los datos personales	DATOS PERSONALES.- Nombre, edad, sexo, firma, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, patrimonio, Clave Única de Registro de Población y lugar de nacimiento. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Nacionalidad, Integrantes de la familia, ingreso familiar mensual, servicios médicos, y familiares con enfermedades crónicas o discapacidad.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento, cada trabajadora social operativa, y administrativa cuentan con los registros propios, para control y seguimiento.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados, en cada espacio físico de las Trabajadoras Sociales. Cada una de ellas cuenta en su espacio físico con un archivero con llave, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento de Trabajo Social, Responsable de la Ventanilla Única del departamento, Recepción del departamento, Trabajadoras Sociales Operativas del departamento, Personal Administrativo que lleva centro de documentos de usuarios; Secretaria del departamento; Coordinadora de CDCS.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de Octubre de 2021.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de la Coord. de Nutrición y Asistencia Alimentaria
Respecto del administrador de éste	**Nombre**	C. Cynthia Maricela Barrera Naranjo
	Cargo	Coordinador de Nutrición y Asistencia Alimentaria
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan

Las funciones y obligaciones de las personas que traten datos personales	•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales	DATOS PERSONALES.- Nombre, fecha y lugar de nacimiento, edad, sexo, nacionalidad, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Única de Registro de Población, RFC, número credencial de elector u otra identificación, estado civil, fotografía, parentescos, familiares o dependientes económicos. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos y preferencia sexual.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero de madera, con llave, asi como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de

seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Coordinadora del departamento; Jefes de área; Secretarias de la coordinación; trabajadores sociales de alimentaria; Auxiliares Administrativos;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	21 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Servicios
Respecto del administrador de éste	**Nombre**	Mtro. Misael Alejandro Simón de la Madrid
	Cargo	Director de Programas
	Adscripción	Dirección de Programas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES: Nombre, edad, sexo, firma, características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Única de Registro de Población (CURP). DATOS PERSONALES SENSIBLES: Adscripción o pertenencia étnica, condición de habla de lengua indígena, estado de salud física y mental, historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, preferencia sexual, condición o situación de derechos vulnerados y procesos de restitución (ej. Adolescentes en conflicto con la ley).
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en la nube (plataforma drive), disco duro de la(s) computadora(s) asignada(s), a la cual solo tiene acceso el personal responsable de la Dirección.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero de madera, con llave, así como en archivos digitales en la nube (plataforma drive), disco duro de la(s) computadora(s) asignada(s) que cuentan con una clave de usuario, a lo cual solo tiene acceso el personal responsable del equipo de cómputo.

Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la falta de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de la Dirección, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay un solo elemento de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Dirección son: • Director(a) de Programas; • Jefe del Departamento de la Delegación Institucional de la Procuraduría de Protección a Niñas, Niños y Adolescentes; • Jefe del Departamento de Protección a la Niñez y Adolescencia; • Jefe del Departamento de Paz y Habilidades Comunitarias; • Jefe de Área B adscrita la Dirección de Programas • Secretaria de Jefe de Departamento adscrita la Dirección de Programas
Procedimientos de respaldo y recuperación de datos personales	Además del archivo físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia.

Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	15 de octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de la Delegación Institucional de la PPNNA
Respecto del administrador de éste	**Nombre**	Lic. Iris Paola Mercado Valdivia
	Cargo	Jefa del Departamento de la Delegación Institucional de la PPNNA
	Adscripción	Dirección de Programas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

Inventario de los datos personales	DATOS PERSONALES: Nombre, edad, sexo, firma, características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Única de Registro de Población (CURP). DATOS PERSONALES SENSIBLES: Adscripción o pertenencia étnica, condición de habla de lengua indígena, estado de salud física y mental, historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, preferencia sexual, condición o situación de derechos vulnerados y procesos de restitución (ej. Adolescentes en conflicto con la ley).
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos digitales en la nube (plataforma drive), disco duro de la(s) computadora(s) asignada(s), a la cual solo tiene acceso el personal responsable del Departamento.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero con llave, así como en archivos digitales en la nube (plataforma drive), disco duro de la(s) computadora(s) asignada(s) que cuentan con una clave de usuario, a lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la falta de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: •JEFE DEL DEPARTAMENTO DE LA DELEGACIÓN INSTITUCIONAL DE LA PROCURADURÍA DE PROTECCIÓN A NIÑAS, NIÑOS Y ADOLESCENTES; • SUBPROCURADOR(A); • SUBPROCURADOR(A); • COORDINADOR(A); • ABOGADOS/AS DEL DEPARTAMENTO • AUXILIARES ADMINISTRATIVOS/AS DEL DEPARTAMENTO • JEFES AREA B DEL DEPARTAMENTO • MEDICOS/AS DEL DEPARTAMENTO • PSICOLOGAS/OS DEL DEPARTAMENTO • SECRETARIAS DEL DEPARTAMENTO • SUPERVISORES DE PROGRAMA • TRABAJADORA(S) SOCIAL
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	15 de ocutbre de 2021

DOCUMENTO DE SEGURIDAD	
Nombre del sistema o base de datos	Base de datos personales del Departamento de Paz y Habilidades Comunitarias

Respecto del administrador de éste	**Nombre**	Mtra. María Zoe Peregrina Aguilar
	Cargo	Jefa del Departamento de Paz y Habilidades Comunitarias
	Adscripción	Dirección de Programas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES: Nombre, edad, sexo, firma, características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Única de Registro de Población (CURP), número de identificación, fecha y lugar de nacimiento, comprobante de ingresos. DATOS PERSONALES SENSIBLES: Fotografía, Adscripción o pertenencia étnica, condición de habla de lengua indígena, estado de salud física y mental, historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, preferencia sexual, condición o situación de derechos vulnerados y procesos de restitución y procesos de restitución preliberados.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en la nube (plataforma drive), disco duro de la(s) computadora(s) asignada(s), a la cual solo tiene acceso el personal responsable del Departamento.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero, con llave, así como en archivos digitales en la nube (plataforma drive), disco duro de la(s) computadora(s) asignada(s) que cuentan con una clave de usuario, a lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos

Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la falta de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: • JEFE DE DEPARTAMENTO • JEFES DE AREA A • JEFE DE ÁREA C • PSICOLOGAS/OS • SECRETARIAS • AUXILIARES ADMINISTRATIVOS DEL DEPARTAMENTO • AUXILIAR DE CENTRO • CONSEJEROS FAMILIARES • TRABAJADORES SOCIALES • SUPERVISORES DE PROGRAMA • EDUCADOR(A) • ADMINISTRADOR(A) DE DEPARTAMENTO • AUXILIAR GENERAL DE DEPARTAMENTO • ODONTÓLOGA (O) • PROMOTORES INFANTILES COMUNITARIOS • PRESTADORES DE SERVICIOS
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	15 de octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de Protección y Adolescencia
Respecto del administrador de éste	**Nombre**	Mtro. Luis Miguel Abundis Camacho
	Cargo	Jefe del Departamento de Protección a la Niñez y Adolescencia
	Adscripción	Dirección de Programas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

Inventario de los datos personales	DATOS PERSONALES: Nombre, edad, sexo, firma, características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Única de Registro de Población (CURP). DATOS PERSONALES SENSIBLES: Adscripción o pertenencia étnica, condición de habla de lengua indígena, estado de salud física y mental, historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, preferencia sexual, condición o situación de derechos vulnerados y procesos de restitución (ej. Adolescentes en conflicto con la ley).
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos digitales en la nube (plataforma drive), disco duro de la(s) computadora(s) asignada(s), a la cual solo tiene acceso el personal responsable del Departamento.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en un archivero con llave, así como en archivos digitales en la nube (plataforma drive), disco duro de la(s) computadora(s) asignada(s) que cuentan con una clave de usuario, a lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la falta de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: • JEFE DE DEPARTAMENTO • AUXILIAR ADMINISTRATIVO DEL DEPARTAMENTO • SECRETARIAS DEL DEPARTAMENTO • JEFES DE AREA • PROMOTORES INFANTILES COMUNITARIOS • PSICOLOGOS/AS • TRABAJADORES SOCIALES • PROMOTORES DEL DEPARTAMENTO
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	15 de ocutbre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de Tutela, Custodia y Adopción
	Nombre	Lic. María Raquel Arias Covarrubias
	Cargo	Coordinadora de Tutela, Custodia y Adopción.

Respecto del administrador de éste	Adscripción	Dirección de Programas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, fecha y lugar de nacimiento, edad, sexo, nacionalidad, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Única de Registro de Población, RFC, número credencial de elector u otra identificación, estado civil, fotografía, parentescos, familiares o dependientes económicos. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero con llave, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos

Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento; Secretarias del departamento; Auxiliares Administrativos;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad	Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.
Programa General de capacitación	

Fecha			Tipo de capacitación	Tipo de personal
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	21 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de la Unidad de Transparencia
Respecto del administrador de éste	**Nombre**	Lic. María Fernanda Canales Espinoza
	Cargo	Jefa de Departamento Titular de la Unidad de Transparencia
	Adscripción	Dirección General
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES: Nombre, fecha y lugar de nacimiento, edad, sexo, firma, domicilio particular, nacionalidad, número de teléfono particular, correo electrónico particular, CURP, RFC, número de credencial de elector y/o documentos de identificación, estado civil, fotografía, cuentas bancarias, parentescos, familiares o dependientes económicos. DATOS PERSONALES SENSIBLES.- historial médico, información genética, afiliación sindical, grado académico, huellas digitales, preferencia sexual.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en drive, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, solo se realiza a correos electrónicos institucionales, que se encuentran publicados en el portal de transparencia de cada sujeto obligado o en el del Instituto de Transparencia, Información pública y Protección de Datos Personales del Estado de Jalisco (ITEI) para cumplir con las obligaciones de transparencia, agregando una constancia de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero con llave, así como en archivos digitales en memoria USB, en drive y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.

Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenen datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en materia de protección de datos personales, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Titular de la Unidad de Transparencia; y Auxiliar del Departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo

Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	19 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Contraloría
Respecto del administrador de éste	**Nombre**	C.P.A. Armando Villalobos González
	Cargo	Contralor
	Adscripción	Contraloría del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y mental e historial médico, afiliación sindical.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada físicamente en expedientes cerrados, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable de la Contraloría

Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes..
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Contraloría son: Contralor; Auditor; y Secretarias de contraloría

Procedimientos de respaldo y recuperación de datos personales	Se cuenta en expediente físico
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	19 de octubre de 2021.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección Jurídica
Respecto del administrador de éste	**Nombre**	Mtra. Ma. Guadalupe Trinidad Castellanos Gutiérrez
	Cargo	Director(a) Jurídico
	Adscripción	Dirección Jurídica del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

Inventario de los datos personales	DATOS PERSONALES.- Nombre, edad, sexo, firma, Características físicas, morales, domicilio particular, número de teléfono particular, Clave Única de Registro de Población, Registro Federal de Contribuyentes, datos de procedimientos jurídicos, bienes muebles o bienes inmuebles, fiscales, ingresos. **DATOS PERSONALES SENSIBLES.- historial médico, afiliación sindical.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable de la Dirección
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero con llave, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Dirección son: Director (a) Jurídico, Abogadas del departamento Auxiliar administrativo o secretaria
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	19 de octubre de 2021.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Planeación
Respecto del administrador de éste	**Nombre**	Lic. Ramsés de Jesús Ascencio Ríos
	Cargo	Director de Planeación
	Adscripción	Dirección de Planeación del Sistema DIF Zapopan

Las funciones y obligaciones de las personas que traten datos personales	•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales	DATOS PERSONALES.- Nombre, edad, sexo, características físicas, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, Clave Única de Registro de Población, datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales. **DATOS PERSONALES SENSIBLES.- Estado de salud física.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual sólo tiene acceso el personal responsable de la Dirección
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero con llave, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Dirección son: Director de Planeación; Jefes de Departamento de Planeación; Jefes de área del departamento ; Estadígrafo del departamento; Auxiliar administrativo del departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tienen los archivos de hojas de cálculo, hojas de texto y demás, en formatos digitales en cuentas asociadas al correo institucional.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de octubre de 2021.

DOCUMENTO DE SEGURIDAD

Nombre del sistema o base de datos		Base de datos personales del Departamento de Planeación Estratégica
Respecto del administrador de éste	**Nombre**	Mtra. Ana Karina Pérez Sánchez
	Cargo	Jefa del Departamento de Planeación Estratégica
	Adscripción	Dirección de Planeación del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, características físicas, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, Clave Única de Registro de Población. **DATOS PERSONALES SENSIBLES.- Estado de salud física.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero con llave, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos

Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento de Planeación Estratégica; Jefes de área del departamento; Estadígrafo del departamento; Auxiliar administrativo y/o secretarias del departamento.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	18 de octubre de 2021.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Administración y Finanzas
Respecto del administrador de éste	**Nombre**	Mtro. Alejandro Acosta Castillo
	Cargo	Director de Administración y Finanzas
	Adscripción	Dirección de Administración y Finanzas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES: Nombre, edad, sexo, firma, características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Única de Registro de Población (CURP), Registro Federal de Contribuyentes (RFC) y cuentas bancarias. DATOS PERSONALES SENSIBLES: Origen racial, condición de habla de lengua indígena, estado de salud física y mental, historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, preferencia sexual, afiliación sindical.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable de la Dirección
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales		Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero de madera, con llave, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.

Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Dirección son: Director de Administración y Finanzas y Secretarias y/o auxiliares de la dirección
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo

Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	19 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de Desarrollo de Capital Humano
Respecto del administrador de éste	**Nombre**	Lic. María Teresa Manzo Melgoza
	Cargo	Jefe del Departamento de Desarrollo de Capital Humano
	Adscripción	Dirección de Administración y Finanzas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES: Nombre, edad, sexo, firma, características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Única de Registro de Población (CURP), cuentas bancarias. DATOS PERSONALES SENSIBLES: Adscripción o pertenencia étnica, condición de habla de lengua indígena, datos biométricos, y parentescos.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento

Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero con llave, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefa del Departamento de Desarrollo de Capital Humano, Secretarias y/o auxiliares del departamento.

Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	19 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de Recursos Financieros
Respecto del administrador de éste	**Nombre**	Mtro. Gabriel Néstor Cárdenas Galván
	Cargo	Jefe del Departamento de Recursos Financieros
	Adscripción	Dirección de Administración y Finanzas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.

Inventario de los datos personales	DATOS PERSONALES: Nombre, edad, sexo, firma, características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Única de Registro de Población (CURP), registro federal de contribuyentes (RFC), datos de identificación y laborales, datos patrimoniales, datos bancarios. DATOS PERSONALES SENSIBLES: Adscripción o pertenencia étnica, condición de habla de lengua indígena, parentescos.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero con llave, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento de Recursos Financieros, Secretarias y/o auxiliares del departamento.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	19 de Octubre de 2021

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Nóminas
Respecto del administrador de éste	**Nombre**	Lic. Nicolás Sandoval Mata
	Cargo	Coordinador de Nóminas
	Adscripción	Departamento de Desarrollo de Capital Humano

Las funciones y obligaciones de las personas que traten datos personales	•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales	**DATOS PERSONALES.-** Nombre, edad, sexo, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Única de Registro de Población, Registro Federal de Contribuyentes, Cuenta Bancaria. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, afiliación sindical.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable de la Coordinación
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero con llave, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Coordinador de Nóminas, Auxiliar administrativo y/o secretarias.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	19 de octubre de 2021.

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Adquisiciones
Respecto del administrador de éste	**Nombre**	Lic. Martha Patricia Quiñonez Pérez
	Cargo	Jefa de Departamento de Compras y Adquisiciones
	Adscripción	Departamento de Recursos Financieros

Las funciones y obligaciones de las personas que traten datos personales	•**Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; •**Abstenerse** de tratar para finalidades distintas a las instruidas; •**Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; •**Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; •**Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; •**Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y •**Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales	DATOS PERSONALES.- Nombre, edad, sexo, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Única de Registro de Población, Registro Federal de Contribuyentes. DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, afiliación sindical, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable de la Coordinación
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en una archivero con llave, así como en archivos digitales en memoria USB, y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos

Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de cómputo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de cómputo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay dos elementos de policía custodiando instalaciones, algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de departamento, y Secretarias y/o auxiliares del departamento.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato PDF de la información que el mismo contiene
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte de la encargada de Protección de Datos Personales de DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia), para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo de capacitación**	**Tipo de personal**
Día	**Mes**	**Año**	Por el momento no lo hay	En su caso será base y confianza que traten datos

Fecha de actualización del documento de seguridad	19 de Octubre de 2021

Controles y mecanismos de seguridad para las transferencias

Transmisiones mediante el traslado de soportes físicos
a) El envío de la información se realiza a través del notificador adscrito al Sistema para el Desarrollo Integral de la Familia del Municipio de Zapopan, Jalisco, o mediante personal autorizado por su superior jerárquico; b) Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utilizara la leyenda de clasificación señalada en los *Lineamientos Generales para Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas*; c) La entrega de información confidencial requiere acuse de recibo, y sólo será entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial

Transmisiones mediante el traslado físico de soportes electrónicos
a) El envío de la información se realiza a través del notificador adscrito al Sistema para el Desarrollo Integral de la Familia del Municipio de Zapopan, Jalisco, o mediante personal autorizado por su superior jerárquico, sin embargo, en este último caso, es necesario contar con oficio de comisión; b) Cuando se transfiere información confidencial esta se realiza en sobres sellados y se utilizara la leyenda de clasificación señalada en los *Lineamientos Generales para Clasificación y Desclasificación de la Información, así como para la Elaboración de las Versiones Públicas*; c) La entrega de información confidencial requiere acuse de recibo, y sólo será entregada a los titulares de la información o sus autorizados, previa acreditación con identificación oficial

Transmisiones mediante el traslado sobre redes electrónicas

a) A partir de la aprobación del presente documento los soportes electrónicos que sean transferidos y contengan información confidencial deberán ser codificados, con el objeto de que únicamente puedan acceder a ellos, las personas que tengan la clave del cifrado.

b) A partir de la aprobación del presente documento las transmisiones deberán ser registradas en las bitácoras de transferencia de cada área.

Bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales

Bitácoras de Acceso

Las bitácoras de acceso a los datos personales deberán contener la siguiente información:

- Nombre y cargo de quien accede
- Identificación del Expediente
- Fojas del Expediente
- Propósito del Acceso
- Fecha y hora de Acceso
- Fecha y hora de Devolución

En ese sentido, las bitácoras de acceso a los datos personales deberán ser resguardadas en archiveros dentro de las instalaciones de al Sistema para el Desarrollo Integral de la Familia del Municipio de Zapopan, Jalisco, a los cuales únicamente tendrán acceso las personas designadas para tal efecto.

El formato de bitácora se encuentra la final del documento como Anexo 1.

Vulneraciones a la Seguridad de los Datos Personales

Cuando exista un intento o bien una vulneración de las medidas de seguridad, este deberá quedar documentado en la bitácora de vulneraciones de seguridad.

La bitácora de vulneraciones deberá contener por lo menos la siguiente información:

1. Nombre, cargo y área del responsable de la investigación;
2. Número de la investigación;
3. Documento vulnerado;
4. Tipo de vulneración;
5. Datos personales vulnerados;
6. Nombre y firma de quien reporta la vulneración.

7. La fecha en la que ocurrió;
8. Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgo

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios distingue en su artículo 38 las siguientes vulneraciones de seguridad de la información confidencial:

- La pérdida o destrucción no autorizada;
- El robo, extravío o copia no autorizada;
- El uso, acceso o tratamiento no autorizado; o
- El daño, la alteración o modificación no autorizada.

Tomando en cuenta las circunstancias generales y actuales, tanto físicas como humanas, de este sujeto obligado donde se tratan los datos personales recabados de las funciones de la administración pública, hemos logrado identificar los siguientes riesgos posibles ante los que se pudiera enfrentar este Sujeto Obligado:

- Recabar de datos incompletos o incorrectos.
- Omitir la notificación al titular de los datos personales del aviso de privacidad.
- No tener a la vista o alcance de los ciudadanos el aviso de privacidad.
- Respecto del consentimiento expreso para el manejo de datos personales: no tener evidencia de que el titular de los datos personales conoce los términos del aviso de privacidad y los acepta.
- No tener las medidas necesarias para garantizar el acceso restringido a los archivos donde se encuentren los datos personales físicamente.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales, sin registros o bitácoras.
- Pérdida de expedientes físicos debido a catástrofes, inundaciones, incendios u otros.
- Daño de la base de datos que contenga información confidencial y datos personales.
- Fallas técnicas en los equipos de cómputo en donde se encuentran las bases de datos.
- Diligencias inadecuadas, malas prácticas de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan y traten debido al desempeño de sus funciones.
- Pérdida, robo o extravío de expedientes integrados con datos personales.
- Alteración de la información respecto a los datos personales.

Ante dichos riesgos identificados es necesario hacer un análisis de dichos riesgos, amenazas y vulneraciones.

Es necesario establecer y evaluar cada uno de los riesgos, partiendo de las amenazas y causas de los riesgos, posteriormente se analizarán los riesgos para poder llegar a las medidas de seguridad aplicables.

Amenazas	Daño
Acceso de personas no autorizadas a los archivos físicos o electrónicos que contengan datos personales, sin fines de lucro.	Acceder a información o datos personales, mediante el acceso no autorizado.
Acceso de personas no autorizadas a los archivos físicos o electrónicos que contengan datos personales, con fines específicos de lucro.	Adquirir información o datos personales. Divulgación de datos personales. Robo de información. Modificaciones no autorizadas. Extorsiones. Ataques a personas. Vulneración a la seguridad física y mental de los ciudadanos.
Diligencias inadecuadas, malas prácticas de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan y traten debido al desempeño de sus funciones.	Obtener información para beneficio personal. Curiosidad. Error involuntario. Por fines económicos.
Daño físico.	Daño o pérdida de los datos personales ocasionados por factores externos como: • Agua. • Fuego. • Accidentes. • Corrosión.
Eventos naturales.	Desastres climatológicos. Fenómenos meteorológicos. Sismos. Cualquier eventualidad por causa natural.
Fallas técnicas.	Pérdida de electricidad. Falla o pérdida de internet. Falla en sistemas, correos electrónicos o plataformas oficiales.
Decadencias técnicas.	Mantenimiento insuficiente. Falla en equipos. Poca o absoluta renovación de equipos de telecomunicaciones o cómputos. Cambios de voltaje.
Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas. Falta de mecanismos para identificar o autenticación de usuarios.

	Falta de actualización de antivirus.
Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.
Espacio donde se archiven.	Carencia de espacio. Espacio con poca seguridad. Espacio no adecuado. Falta de llaves o medidas de seguridad para accesos.
Daño y/o alteración de la base de datos que contenga información confidencial.	Carencia de un servidor o sistema que almacene los datos personales. La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos personales y la pérdida, robo o extravío de expedientes.

Análisis de brecha

Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base los inventarios de datos personales que se hicieron con cada área de al Sistema para el Desarrollo Integral de la Familia del Municipio de Zapopan, Jalisco.

Las diferentes direcciones reportaron las siguientes medidas de seguridad existentes:

- Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios, únicamente los necesarios derivados del ejercicio de sus atribuciones y facultades.
- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones y en espacios asignados para archivo.
- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.
- En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir si fue recabado frente a un escritorio, área abierta o pasillo, los

ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos.

- La oficina cuenta con puertas que separa el área al momento de terminar labores.
- Las llaves que se tienen de la oficina se encuentran en manos de servidores públicos, autorizados por el área general.
- Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.
- Una vez recabados los datos personales, ya realizada la carpeta o expediente (electrónica, física, en plataformas, o cualquiera generada) y guardada esta en archiveros o puesta en resguardo electrónico, tienen acceso a esta área servidores públicos del área.
- Las llaves de los archiveros con las que se cuentan se encuentran en posesión de servidores públicos encargados del área.
- Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.
- Durante el desahogo del trámite del cual se obtuvieron los datos personales, los servidores públicos del área tienen acceso a los datos personales.
- Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.
- Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área.
- El aviso de privacidad se encuentra a la vista y alcance de los ciudadanos, es decir en el espacio físico donde se recaban los datos personales.

Aunado a la existencia de las medidas de seguridad anteriormente enlistadas es de suma importancia de dar continuidad a las mismas, ya que son la base mínima para garantizar el resguardo y protección de la información confidencial y datos personales, además de que se han convertido en procedimientos y prácticas ya establecidas normativamente, no obstante las medidas de seguridad son adquiridas por parte del personal en el desempeño de sus funciones en cada área, como buena práctica, lo cual hace más fácil mantenerlas a lo largo del tiempo.

Partiendo de la existencia y aplicación de las medidas de seguridad, existe la necesidad de establecer nuevas medidas de seguridad, de conformidad con la evolución y necesidades que se presentan a lo largo del tiempo, estas con el fin de aplicar medidas de seguridad estandarizadas para todas y cada una de las áreas que recaben, administren o traten datos personales.

Derivado de la implementación y actualización de las medidas de seguridad existe una necesidad de difusión y capacitación en materia de protección de datos personales al interior de este Sujeto Obligado.

La constante actualización de medidas de seguridad y la capacitación de los servidores públicos es necesaria para el adecuado trato de los datos personales. No obstante, este documento está orientado a llenar esos vacíos y servir como un instrumento de observancia general dentro de este sujeto obligado, que ayudará a dar cumplimiento con las disposiciones en materia de datos personales.

Gestión de vulneraciones

Plan de respuesta

1) Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos;

2) El personal del Sistema para el Desarrollo Integral de la Familia del Municipio de Zapopan, Jalisco, que detecte la vulneración deberá proceder al llenado del Formato relativo a Vulneraciones a los Sistemas de Información y Bases de Datos, mismo que se adjunta al final como anexo 2.

3) Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.

4) Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales.

5) En caso de que la vulneración fuera resultado de la comisión de un delito se presentaran las denuncias correspondientes ante las autoridades competentes, a través de la Dirección Jurídica del Sistema para el Desarrollo Integral de la Familia del Municipio de Zapopan, Jalisco.

Medidas de seguridad implementadas

Medidas de Seguridad Físicas

La seguridad física consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial,

es decir, se refiere a los controles y mecanismos de seguridad dentro y alrededor de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo, con el objeto de prevenir accesos no autorizados, daños, robos, entre otras amenazas.

Entorno Institucional:

Se cuenta con elementos de seguridad en la entrada de este Sujeto Obligado;

Se cuenta con cámaras de video vigilancia por fuera y dentro de este Sujeto Obligado.

Entorno de los datos

- No se sitúan equipos en sitios altos para evitar caídas,
- No se colocan elementos móviles sobre los equipos para evitar que caigan sobre ellos;
- Se cuenta con equipo para la extinción de incendios;
- Se prohíbe el uso o consumo de líquidos sin tapa alrededor de los equipos para evitar que caigan sobre ellos;
- Se hacen copias de seguridad semanales de los documentos electrónicos.

Controles de identificación y autenticación de usuarios

Los empleados del Sistema para el Desarrollo Integral de la Familia del Municipio de Zapopan, Jalisco, deben portar en todo momento su identificación institucional vigente, el cual deberá contar por lo menos con la siguiente información:

Al frente del gafete:

- Nombre; y
- Cargo.

Al reverso del gafete:

- Vigencia;
- Número y firma del empleado;
- Domicilio de la institución; y
- Teléfono de la institución.

Ahora bien, en el ambiente electrónico todas las computadoras deberán contar con usuario y contraseña para ingresar, asimismo, los usuarios al dejar de utilizar una computadora deberán bloquear las pantallas de sus equipos electrónicos, con el objeto de evitar posible robo de información.

Aunado a ello, las contraseñas de los equipos electrónicos deberán ser modificadas por los usuarios cada 06 seis meses.

Asimismo, los ciudadanos que ingresen a las instalaciones deberán registrarse en la entrada, en la que deben señalar por lo menos los siguientes datos;

- Nombre;
- Área a la que se dirige;
- Motivo de su visita;
- Día hora y fecha; y
- Número de identificación oficial, siempre y cuando sea necesario que el ciudadano acredite su identidad ante el sujeto obligado.

Procedimientos de respaldo y recuperación de datos personales

Respaldo

Se realiza una digitalización completa de la información que ingresa y se almacena en discos duros.

Recuperación

Los respaldos incrementales contienen fecha y hora, tanto inicial como final. La recuperación se realiza cruzando la fecha del incidente y el último respaldo.

Técnicas de Supresión y Borrado Seguro de Datos Personales

Métodos Físicos

1. Trituración mediante corte cruzado o en partículas: Cortar el documento de forma vertical y horizontal generando fragmentos diminutos, denominados “partículas”, lo cual hace prácticamente imposible que se puedan unir.

2. Destrucción de los medios de almacenamiento electrónicos mediante desintegración, consistente en separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.

Métodos Lógicos

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

Eliminación del documento: consiste en suprimir el documento de la computadora, de la papelera de reciclaje y, en su caso, del respaldo que hubiera.

Plan de trabajo

La existencia del documento de seguridad, busca enmarcar los deberes del **Sistema para el Desarrollo Integral de la Familia del Municipio de Zapopan, Jalisco,** para la óptima protección de datos personales; en ese sentido, debido a la importancia en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad.

Con base en lo anterior, se ha planteado implementar la totalidad de las medidas de seguridad faltantes en un periodo de dieciocho meses a partir de la aprobación del presente documento de seguridad; con base en lo anterior, las medidas de seguridad físicas y técnicas que requieran la erogación de recursos, se realizarán conforme a los tiempos administrativos y el presupuesto lo permita.

Para la ejecución del presente documento de seguridad, se dará prioridad a las siguientes actividades:

Mes 1 al 6

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 del Sistema para el Desarrollo Integral de la Familia del Municipio de Zapopan, Jalisco.

2. Se solicitará apoyo del *Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco*, para la capacitación de los servidores públicos que recaban datos personales;

Mes 7 al 12

1. Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad;

Mecanismos de monitoreo y revisión de las medidas de seguridad

Se debe realizar un monitoreo y revisión de la aplicación de las medidas de seguridad, para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización; esto con el objeto de que las medidas de seguridad continúan siendo efectivas e idóneas; en consecuencia, **se deberá realizar informes anualmente**.

Programa General de Capacitación

Se manejarán las capacitaciones de conformidad con las necesidades del sujeto obligado en cuanto a la implementación y aplicación del sistema de manejo de datos personales, en posesión del sujeto obligado, entre los temas a capacitar se encuentran los siguientes:

- Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados;
- Principios y deberes que deben observarse en el tratamiento de los datos personales; y
- Sistema de Gestión, Medidas de seguridad

Anexo 1

Bitácora de Acceso					
Nombre y cargo de quien accede	Identificación del Expediente	Fojas del Expediente	Propósito del Acceso	Fecha y hora de Acceso	Fecha y hora de Devolución

Anexo 2

Bitácora de vulneraciones									
NOMBRE DEL RESPONSABLE DE LA INVESTIGACIÓN	CARGO	AREA	NÚMERO DE INVESTIGACIÓN	SISTEMA(S(DE INFORMACIÓN O BASE(S) DE DATO(S) VULNERAD(O)	TIPO DE VULNERACIÓN	TIPO DE DATOS PERSONALES COMPROMETIDOS	Nombre y firma de quién reporta	Fecha en la que ocurrió	Medidas correctivas

Anexo 3

Bitácora de Transferencias

Fecha	Medio	Datos Personales Transferidos	Receptor	Persona que recibe	Autorización

Anexo 4

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, que nos permita dar continuidad a la aplicación de este documento de seguridad, así como enfrentarnos a fallas y eventos inesperados que podrían derivar en la pérdida parcial o total de la información confidencial que posee este sujeto obligado.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones y daños a los 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 existen riesgos inminentes que día a día evoluciona.

En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia.

En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo.