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	Olga María Esparza Campa
	Cargo	Directora 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, referencia sexual, Clave Unica 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 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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora 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 policia que resguarda las instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	El usuario que tratan información en esta Dirección son Olga María Esparza Campa, Directora de Administración y Finanzas.
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018

Departamento de Desarrollo de Capital Humano

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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**	Gabriela Soledad Ramírez Rodríguez
	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, referencia sexual, Clave Unica 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 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, 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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 un solo elemento de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora 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 policia que resguarda las instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	El usuario que tratan información en este Departamento son Gabriela Soledad Ramírez Rodriguez, Jefe del Departamento de Desarrollo de Capital Humano.
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018

Departamento de Recursos Financieros

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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**	Juan Crisóstomo Rodríguez Sustaita
	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, referencia sexual, Clave Unica 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 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, 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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 un solo elemento de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora 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 policia que resguarda las instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	El usuario que tratan información en este Departamento son Juan Crisóstomo Rodríguez Sustaita, Jefe del Departamento de Recursos Financieros
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018

Coordinación de Adquisiciones

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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**	Beatriz Angelica Pimentel Gutiérrez
	Cargo	Coordinador de 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, referencia sexual, Clave Unica 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 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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de la Coordinación, 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 policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora 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 policia que resguarda las instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Coordinación, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	El usuario que tratan información en esta Coordinación son Beatriz Angelica Pimentel Gutiérrez Coordinador de Adquisiciones.
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018

Coordinación de Nóminas

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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	Elizabeth Guadalupe Barboza González
	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, referencia sexual, Clave Unica 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 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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de la Coordinación, 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 policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora 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 policia que resguarda las instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Coordinación, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	El usuario que tratan información en esta Coordinación son Elizabeth Guadalupe Barboza González, Coordinador de Nóminas.
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018

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**	Mtra. Diana Berenice Vargas Salomón
	Cargo	Directora 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, actual Jefe de Departamento Titula de la Unidad de Transparencia; • **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 (Jefe de Departamento Titula de la Unidad de Transparencia), 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 (Jefe de Departamento Titula de la Unidad de Transparencia), así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente del municipio o estatales tales como Sistema DIF Estatal, Autoridades del Sistema de Justicia, Fiscalía General del Estado.
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		A partir de este momento, 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, 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 elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 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 metálica con cristal y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Dirección son: • Diana Berenice Vargas Salomón, Directora de Programas; • Evangelina Cázares Ruiz, Jefe del Departamento de la Delegación Institucional de la Procuraduría de Protección a Niñas, Niños y Adolescentes; • Ernesto Cisneros Priego, Jefe del Departamento de Protección a la Niñez y Adolescencia; • León Delgadillo Rosas, Jefe del Departamento de Paz y Habilidades Comunitarias; • Gizela Pinedo Pérez, Jefe de Área B adscrita la Dirección de Programas • Nora Karina Camacho Miramontes, 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.

Gobierno de Zapopan | Ciudad de los niños

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DIF Zapopan

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**	Evangelina Cazarez Ruíz
	Cargo	Jefe 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, actual Jefe de Departamento Titula de la Unidad de Transparencia; • **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 (Jefe de Departamento Titula de la Unidad de Transparencia), 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 (Jefe de Departamento Titula de la Unidad de Transparencia), así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente del municpio o estatales tales como Sistema DIF Estatal, Autoridades del Sistema de Justicia, Fiscalía General del Estado.
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 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		A partir de este momento, 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, 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 elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 un solo elemento de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora 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 policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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	León Delgadillo Rosas
	Cargo	Jefe 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, actual Jefe de Departamento Titula de la Unidad de Transparencia; • **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 (Jefe de Departamento Titula de la Unidad de Transparencia), 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 (Jefe de Departamento Titula de la Unidad de Transparencia), así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente del municipio o estatales tales como Sistema DIF Estatal, Autoridades del Sistema de Justicia, Fiscalía General del Estado.	
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 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		A partir de este momento, 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, 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 elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 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 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 metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
	Los usuarios que tratan información en este Departamento son: • DELGADILLO ROSAS LEON, JEFE DE DEPARTAMENTO • CARRILLO RUBIO DIANA JACQUELINE, JEFE DE AREA A • FLORES LOPEZ PAULINA, JEFE DE ÁREA C • JAUREGUI ARANA BERTHA ALICIA, PSICOLOGO(A) • GUIZAR BARRIGA ESTRELLA URUAPAN, SECRETARIA DE JEFE DE DEPARTAMENTO • MUÑOZ FREGOSO SILVIA, SECRETARIA DE JEFE DE DEPARTAMENTO • JUAREZ RENDON ELIZABETH, AUXILIAR ADMINISTRATIVO • HERNANDEZ AVALOS ENRIQUE, AUXILIAR ADMINISTRATIVO • BRAMBILA GONZALEZ CRISTINA, AUXILIAR DE CENTRO • MARTINEZ OLVERA CLEMENCIA ROCIO, CONSEJERO FAMILIAR • HERNANDEZ MORAN MARIA DEL PILAR, CONSEJERO FAMILIAR • SANCHEZ GIL NORA ELBA, PSICOLOGO(A) • ROMERO LEMUS SERGIO, PSICOLOGO(A) • GONZALEZ GARCIA MILDRED, PSICOLOGO(A) • BOGARIN VAZQUEZ MARIA MARTHA, PSICOLOGO(A) • CORONA GONZALEZ CECILIA, PSICOLOGO(A) • TORRES DELGADILLO MARIA YOLANDA, PSICOLOGO(A) • HERNANDEZ RAMOS MARTHA ARACELI, PSICOLOGO(A) • QUEZADA ORTIZ MARTHA ELIZABETH, PSICOLOGO(A) • BRISEÑO GARCIA MARTHA, PSICOLOGO(A) • BECERRA ALONSO BRENDA RUBI, PSICOLOGO(A)

Gobierno de Zapopan | Ciudad de los niños

Departamento de Protección a la Niñez y Adolescencia

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DIF Zapopan

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**	Ernesto Cisneros Priego
	Cargo	Jefe del Departamento de Protección 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, actual Jefe de Departamento Titula de la Unidad de Transparencia; • **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 (Jefe de Departamento Titula de la Unidad de Transparencia), 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 (Jefe de Departamento Titula de la Unidad de Transparencia), así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente del municpio o estatales tales como Sistema DIF Estatal, Autoridades del Sistema de Justicia, Fiscalía General del Estado.	
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 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		A partir de este momento, 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, 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 elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 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 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 metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.

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 Berenice Carabez Hernández
	Cargo	Contralora
	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 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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, 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, 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 elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de la Contraloría, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; los archiveros tienen chapa; hay un solo elemento de policía custodiando instalaciones, algunos equipos de computo 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 metálica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Contraloría, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archiveros de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Contraloría son Berenice Carabez Hernández , Contralora y Carlos Vázquez López Auditor
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018

Departamento del Centro Metropolitano del Adulto Mayor

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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 Gonzalez
	Cargo	Jefe 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, edad, sexo, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Unica de Registro de Población. **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 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, 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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 un solo elemento de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora 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 policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son María Guadalupe Díaz González, Jefe del Departamento del Centro Metropolitano del Adulto Mayor, M. Leticia Dueñas Plascencia, Secretaria; Lurdes Adriana García Torres, Auxiliar Administrativo; Socorro Angélica Alcalá Mendoza, Secretaria; María de la Paz Rodríguez Sánchez, Secretaria; Itzia Citlalli Vázquez Aldama, Secretaria; Ana Luisa España Fernández, Trabajadora Social; Leticia Guadalupe Romero Lima, Trabajadora Social; Celia Cruz Rubio Romero, Trabajadora Socia; Aurora Villa Mascorro, Trabajadora Social; Héctor Daniel Nuño Guitiérrez, Abogado; Mayra González Mora, Trabajadora Social; Bertha Alicia Villanueva Villalobos, Trabajadora Social; Francisco Javier Márquez Campos, Médico General; Jaime Ríos Ramírez, Psicólogo; Ana Alejandra Cervantes Díaz, Enfermera; Jessica Elena Prado Ballardo, Odontóloga; Verónica Iñiguez Reyes, Odontóloga; y José Humberto Ramírez Mora, Podólogo;
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018

Ciudad de los niños

Departamento de Autismo

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de Autismo
Respecto del administrador de éste	**Nombre**	Ruth Araceli Reyes Melchor
	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, edad, sexo, fecha de nacimiento, nombre de los tutores, vida afectiva familiar, vida escolar, domicilio particular, número de teléfono particular, correo electrónico particular. **DATOS PERSONALES SENSIBLES.- Diagnóstico médico, Estado de salud física y mental, historial médico, estudios neurológicos, evaluación de desarrollo de habilidades, reporte de avances terapéuticos.**
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 una archivero de madera, con llave, 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		A partir de este momento, 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, 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 elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 un solo elemento de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas 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 policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta de cristal con chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con dos puertas, la primera de madera con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son Ruth Araceli Reyes Melchor, Jefe del Departamento de Autismo; Anira Montes Cid, Educadora; Eva Maria Zalpa Gómez, Psicóloga; Cinthya García Martínez, Psicóloga; Martha Minerva Gutiérrez Martínez, Psicóloga; Paola Arana Palencia, Educadora; Sandra Patricia Velázquez Guerra, Psicóloga; Martha Vázquez Lara, Psicóloga; Hilda Anahí Valadez Flores, Educadora; María Zenyasse Flores Aceves, 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018

Departamento de Salud y Bienestar

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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**	Ma. Soveida Martínez Campos
	Cargo	Jefe del Departamento 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, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, referencia sexual, Clave Unica de Registro de Población,**DATOS PERSONALES SENSIBLES.- Estado de salud física y mental e historial médico, información genética, datos biométricos.**
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, 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 cajas de cartón, en un salón del Centro de Desarrollo Comunitario "Miramar" , 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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran resguardados en cajas de cartón, en un salón del Centro de Desarrollo Comunitario "Miramar" , mismo que cuenta con llave a cargo de la administradora asignada a ese Centro de Desarrollo Comunitario mencionado, pero carecen de Seguridad, ya que no se cuenta con policia que custodie las instalaciones; algunos equipos de computo son obsoletos y carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora 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	Actualmene estamos en espera de la asignación de un espacio fisico, para el resguardo de los expedientes, debido a la rehabilitación del edificio.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son Ma. Soveida Martinez Campos, Jefe del Departamento de Salud y Bienestar; Laura Elena Cabral Rodríguez, Médico general; Ma. Isabel Figueroa Fierro, Trabajadora Social; Gloria Emma Guerrero Espinoza; Trabajadora social; Ma de Jesús Rico García, Trabajadora Social, Jose Luis Gil Aguilar, Trabajador Social; Aída Gabriela Briones Gutiérrez, Auxiliar Administrativo; Irma Letisia Cortés Sosa; Secretaria Jefe de Departamento, Maria del Refugio Torres Gonzalez, Secretaria.
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018

Coordinación de Centros de Atención

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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 Mejia
	Cargo	Jefa de Area
	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 economicos, correo electrónico particular, Ocupación, Escolaridad, Clave Unica 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 una archivero de madera, 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 una archivero de madera, con llave, asi 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		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 recientemente se implementó la bitacora 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	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 Lic. Natalia Eugenia Ruelas Mejia Jefa de Area, Lic. Bertha Alicia Arechiga Mendoza Trabajadora Social, Lic. Teresa Pimentel Bojorquez Psicologa, Dr. Camarillo Luevano Estela Medico General.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	26 de Julio de 2018

Gobierno de Zapopan | Ciudad de los niños

Coordinación de Centros de Atención

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DIF Zapopan

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. Mildred Marimar Martinez Sanchez
	Cargo	Jefa de Area
	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 economicos, correo electrónico particular, Ocupación, Escolaridad, Clave Unica 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 una archivero de madera, 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 una archivero de madera, con llave, asi 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		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 recientemente se implementó la bitacora 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	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 Lic. Mildred Marimar Martinez Sanchez Jefe de Area, Lic. Rosa Ma. Pulido Guareño Trabajadora Social, Lic. Azucena González Barreto Psicologa, Dr. Hernandez Vazquez Maria Cristina Medico General del centro.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	26 de Julio de 2018

Coordinación de Centros de Atención

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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. Maria del Carmen Karina Soria Hernandez
	Cargo	Jefa de Area
	Adscripción	Centros de Atenciòn
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 economicos, correo electrónico particular, Ocupación, Escolaridad, Clave Unica 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 una archivero de madera, 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 una 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		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 recientemente se implementó la bitacora 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	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 sonLic. Maria del Carmen Karina Soria HernandezJefe de Area, Lic. Lorena Peña Meza Trabajadora Social, Lic. Juana Verónica Gutiérrez Cruz Psicologa, Medina Hernandez Maria Trinidad Medico.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	26 de Julio de 2018

Gobierno de Zapopan | Ciudad de los niños

Coordinación de Centros de Atención

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DIF Zapopan

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 Area
	Adscripción	Centros de Atenciòn
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 economicos, correo electrónico particular, Ocupación, Escolaridad, Clave Unica 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 una archivero de madera, 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 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		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 recientemente se implementó la bitacora 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	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 y Lic. Mónica Gómez Meza Jefa de Area, Lic. Miriam Olivares Cervantes Trabajadora Social, Lic. Melina Esmeralda Ortega Torres Psicologa, Dr. Sandoval Miramontes Maria Soledad Medico General.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	26 de Julio de 2018

Gobierno de Zapopan | Ciudad de los niños

Coordinación de Centros de Atención

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DIF Zapopan

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. Nohemi Edith Salazar Gutierrez
	Cargo	Jefa de Area
	Adscripción	Centros de Atenciòn
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 juridicos 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 economicos, correo electrónico particular, Ocupación, Escolaridad, Clave Unica 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 fisicos en una archivero de madera, 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 una archivero de madera, con llave, asi 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		A partir de este momento, se elaborò la bitacora 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, 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 elaborò la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 recientemente se implementó la bitacora 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	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 Lic. Nohemi Edith Salazar Gutierrez Jefe de Area, Lic. Irma Gabriela Garcia Torrez Trabajadora Social, Lic. Laura Imelda Becerra Psicologa, Dr. Gutierrez Tinoco Maria Dolores Medico General.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	26 de Julio de 2018

Ciudad de los niños | Coordinación de Centros de Atención

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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. Mirna Alvarez Rojo
	Cargo	Jefa de Area
	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 economicos, correo electrónico particular, Ocupación, Escolaridad, Clave Unica 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 una archivero de madera, 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 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		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió: Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 recientemente se implementó la bitacora 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	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 Lic. Ma. Mirna Alvarez Rojo Jefe de Area, Lic. Martha Alicia Hernández García Trabajadora Social, Lic. Norma Angélica Margarito Juárez Psicologa, Dra.Maria Patricia Gómez Plascencia, Médico General.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	26 de Julio de 2018

Ciudad de los niños

Coordinación de Centros de Atención

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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 Esther Ornelas Fuentes
	Cargo	Jefa de Area
	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 economicos, correo electrónico particular, Ocupación, Escolaridad, Clave Unica 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 una archivero de madera, 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 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		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 recientemente se implementó la bitacora 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	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 Rosa María Torres Guzmán, Coordinador de Centros de Atención y Lic. María Esther Ornelas Fuentes Jefe de Area, Lic. Lucía del Carmen Cárdenas Rodriguez Trabajadora Social, Psi. Ema Valdominos Rosales Psicologa, Velazquez Santana Sergio, Médico del centro.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	26 de Julio de 2018

Gobierno de Zapopan | Ciudad de los niños

Coordinación de Centros de Atención

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DIF Zapopan

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. Beatriz Arcelia González López
	Cargo	Jefa de Area
	Adscripción	Centros de Atenciòn
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 juridicos 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, asi 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 economicos, correo electrónico particular, Ocupación, Escolaridad, Clave Unica 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 una archivero de madera, 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 una archivero de madera, con llave, asi 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		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 recientemente se implementó la bitacora 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	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 Lic. Beatriz Arcelia González López Jefe de Area, Lic. María Candelaria Hernández Rodriguez Trabajadora Social, Lic. Cecilia Valle Cervantes Psicologa, Dr. Gutierrez Herrera Leobardo Medico General.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	26 de Julio de 2018

Gobierno de Zapopan | Ciudad de los niños

Coordinación de Centros de Atención

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DIF Zapopan

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. Nancy Castillo Miranda
	Cargo	Jefa de Area
	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 economicos, correo electrónico particular, Ocupación, Escolaridad, Clave Unica 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 una archivero de madera, 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 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		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 recientemente se implementó la bitacora 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	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 Lic. Nancy Castillo Miranda Jefe de Area, Lic. Maria de la Luz Arambul Martínez Trabajadora Social, Lic. María de Jesús Viveros Susunaga Psicologa, Dr. Bravo Pozos Oscar Medico General.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	26 de Julio de 2018

Gobierno de Zapopan | Ciudad de los niños

Coordinación de Centros de Atención

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DIF Zapopan

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 Area
	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 economicos, correo electrónico particular, Ocupación, Escolaridad, Clave Unica 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 una archivero de madera, 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 de madera, con llave, asi 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		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 recientemente se implementó la bitacora 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	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 Lic. Ruth Verónica Sánchez Solano Jefa de Area, Lic. Roselia Limón Castro Trabajadora Social, Lic. Verónica Alcazar Zepeda Psicologa, Dr. Primitivo Diaz Garcia Médico General.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	26 de Julio de 2018

Coordinación de Autismo

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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**	María Zenyasse Flores Aceves
	Cargo	Coordinador 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, edad, sexo, firma, vida afectiva familiar, domicilio particular y número de teléfono particular. DATOS PERSONALES SENSIBLES.- **Estado de salud física y mental e historial médico, información genética.**
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 diagnósticos físicos, se encuentran numerados y resguardados en una 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		A partir de este momento, 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, 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 elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en un archivero de madera con número de inventario 26841 de la Coordinación, para evitar que el personal del Organismo no autorizado, tenga acceso a ellos; el archivero tiene chapa, sin embargo se encuentra fuera de las instalaciones de DIF (CAM José Vasconcelos adscrito a la SEP).

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora 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	Para ingresar a la oficina de la Coordinación, se cuenta con una puerta de madera sin chapa de seguridad y en el interior de ella se tiene el archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son María Zenyasse Flores Aceves Coordinador de Autismo y Ruth Araceli Reyes Melchor Jefe de Departamento de Autismo.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia en word 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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018

Ciudad de los niños

Departamento de Trabajo Social

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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**	Dora Aida Vargas Ocegueda
	Cargo	Jefe 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, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, Clave Unica de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Nacionalidad, Datos generales desu domicilio con cruces y colonia, asi como municipio de nacimiento, y residencia dentro del mismo, telefono particular y uno adicional donde dejar recados, Integrantes de la familia, ingreso familiar mensual, servicios medicos, y familiares con enfermedades cronicas 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, 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 cada espacio físico de las Trabajadoras Sociales que acontinuacion se mencionan: Nora Gabriela Mercado, Ma. Concepcion Flores Lira, Celia Romero Angeles, Alina Karela Miranda, Araceli Leticia Salazar Ibarra, y Angela Torres Molina, cada una de ellas cuenta en su espacio físico con un 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
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo y de respaldo seguro de información, (medidas de seguridad técnicas). Existe el gran riesgo de que los expedientes se encuentren bajo su resguardo, ya que en ocaciones que no acuden a laborar y los ususarios se presentan, por lo que sera necesario trasladarlos a un area comun,

Análisis de brecha
Los expedientes se encuentran en archiveros del Departamento, donde cada Trabajadora Social los resguarda por lo que se considera conveniente, contar con llaves dobles, donde la jefatura/ Direccion de area debera tener bajo su resguardo, asi como un listado mensual actualizado a fin de lograr brindar un optimo servicio a la ciudadania, y por ende a la autoridad que requiera de algun expediente.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementara una bitacora de control y salida de expedientes (Es importante aclarar, quedesde Marzo del 2017 se propuso realizar este control ,sin éxito debido a la queja manifestada del personal operativo de este departamento a travez de acta levantada en el area juridica de este mismo organismo

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policia que resguarda las Instalaciones y controla ingresos a las mismas sin embargo debera contar con apoyo para rondines por las diversas areas, a fin de verificar constantemente a las personas que ingresan con actitudes sospechosas.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son Dora Aida Vargas Ocegueda, Jefe del Departamento de Trabajo Social , Maria del Carmen Rubi responsable de la Ventanilla Unica, Maria Elena Villalpando Recepcion, Trabajadoras Sociales Operativas: Nora Gabriela Mercado, Araceli Leticia Salazar,Alina Karela Miranda, Celia
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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
26	7	2018		
Fecha de actualización del documento de seguridad			26 de Julio de 2018	

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. Carlos Edu Nuño Carranza
	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, firma, 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 y mental.**
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 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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, 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, 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 elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 computo 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 metálica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Dirección son Carlos Edu Nuño Carranza, Director de Planeación; Jorge Iván Segura Michel, Jefe de Departamento de Planeación; Fernanda Torres Alvarado, jefa de área; José Jairo Alvarado Cisneros jefe de área; Patricia Luis Rodríguez jefa de área, Jésus Diaz Valdivia, estadígrafo y Erendira Bejarano Cázares, auxiliar administrativo.
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	26 de Julio de 2018

Departamento de Planeación Estratégica

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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**	Jorge Iván Segura Michel
	Cargo	Jefe del Departamento de Planeación Estratégica
	Adscripción	Dirección de Planeción 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, 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 y mental.**
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, 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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo 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 un solo elemento de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora 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 policia que resguarda las instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Departamento, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son Jorge Iván Segura Michel, Jefe del Departamento de Planeación Estratégica y Fernanda Torres Alvarado, jefa de área; José Jairo Alvarado Cisneros jefe de área; Patricia Luis Rodríguez jefa de área, Jésus Díaz Valdivia, estadígrafo y Erendira Bejarano Cázares, auxiliar administrativo.
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección Jurídica
Respecto del administrador de éste	Nombre	Mtro. Lis Alberto Castro Rosales
	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 PERSONALES SENSIBLES.- historial médico, información genética, afiliación sindical, creencias religiosas.**
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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, 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, 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 elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 de un mantenimiento eficaz a equipos de computo 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 computo 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 computo 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 metálica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Dirección son Luis Alberto Castro Rosales, Director Jurídico, Yolanda Vazquez Fernandez y Paula Ivette Sánchez Vázquez Abogadas.
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	24 de Julio de 2018

Departamento de la Unidad de Transparencia

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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**	Miguel Escalante Vazquez
	Cargo	Jefe de Departamento Titular de la Unidad de 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		Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, correo electrónico particular.
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, 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 de madera, 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 computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora 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, 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 elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada 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 computo 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 computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de la oficina Departamental, pero los usuarios y personal del Organismo tienen acceso a ellas; los archiveros tienen chapa, pero carecen de llave; hay un solo elemento de policia custodiando instalaciones, los equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora 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 policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas del modulo "D" se cuenta con una puerta metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además para ingresar a la oficina del Departamento de la Unidad de Transparencia, se cuenta con otra puerta de madera, con doble chapa de seguridad y en el interior de ella se tiene un archivero de madera en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Miguel Escalante Vazquez, Titular de la Unidad de Transparencia, usuario único de la Información que se trata.
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
De forma bimestral 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 al Responsable de Protección de Datos Personales del Sistema DIF Zapopan.

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	27 de Julio de 2018