Contraloría

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Contraloría
Respecto del administrador de éste	**Nombre**	Ing. Felipe Valdez de Anda
	Cargo	Contralor
	Adscripción	Contraloría del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.- Estado de salud física y mental e historial médico, afiliación sindical.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada fisicamente 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		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta 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 Contraloria, 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: Contralor; Auditor; y Secretarias de contraloría
Procedimientos de respaldo y recuperación de datos personales	Se cuenta el expediente físico y digitalizado
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

Fecha de actualización del documento de seguridad	21 de noviembre de 2024

Dirección de Administración y Finanzas

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Administración y Finanzas
Respecto del administrador de éste	**Nombre**	Mtro. Alejandro Acosta Castillo
	Cargo	Director de Administración y Finanzas
	Adscripción	Dirección de Administración y Finanzas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES: Nombre, edad, sexo, firma, características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Única de Registro de Población (CURP), Registro Federal de Contribuyentes (RFC) y cuentas bancarias. DATOS PERSONALES SENSIBLES: Origen racial, condición de habla de lengua indígena, estado de salud física y mental, historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, preferencia sexual, afiliación sindical.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable de la Dirección
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, 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 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		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha 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	Los usuarios que tratan información en esta Dirección son: Director de Administración y Finanzas, Secretarias de la dirección y Asistente de la dirección
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

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

Fecha de actualización del documento de seguridad	21 de noviembre de 2024

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

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha 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: Jefe del Departamento de Desarrollo de Capital Humano, Secretarias del departamento.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

Fecha de actualización del documento de seguridad	21 de noviembre de 2024

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

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha 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: Jefe del Departamento de Recursos Financieros, Secretarias del departamento.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

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

Fecha de actualización del documento de seguridad	21 de noviembre de 2024

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**	Lic. Maria de Lourdes Corona Gutiérrez
	Cargo	Coordinador de Nóminas
	Adscripción	Departamento de Desarrollo de Capital Humano
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.-** Nombre, edad, sexo, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Unica de Registro de Población, Registro Federal de Contribuyentes, Cuenta Bancaria. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, afiliación sindical, 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, 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 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		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha 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	Los usuarios que tratan información en esta Coordinación son: Coordinador de Nóminas, Auxiliar Adminsitrativo.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

Fecha de actualización del documento de seguridad	21 de noviembre de 2024

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**	Lic. Martha Patricia Quiñonez Pérez
	Cargo	Jefa de Departamento de Compras y Adquisiciones
	Adscripción	Departamento de Recursos Financieros
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave 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, 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 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		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha 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	Los usuarios que tratan información en esta Coordinación son: Jefe de departameto de compras y adquisiciones, Secretarias del departamento.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

Fecha de actualización del documento de seguridad	21 de noviembre de 2024

Departamento de Servicios Generales

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de Servicios Generales
Respecto del administrador de éste	**Nombre**	Arq. Felipe de Jesús García Andrade
	Cargo	Jefe del Departamento de Servicios Generales
	Adscripción	Dirección de Administración y Finanzas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Unica de Registro de Población, Registro Federal de Contribuyentes, datos laborales, patrimoniale, datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales, datos academicos, de transito o movimientos migrtorios. **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, 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 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		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha 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: Jefe del Departamento de Servicios Generales, Secretarias del departamento.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

Fecha de actualización del documento de seguridad	21 de noviembre de 2024

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

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 se cuenta con 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 no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta 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 metalica, 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: Director de Planeación; Jefes de Departamento de Planeación; Jefes de área del departamento ; Estadígrafo del departamento; Auxiliar administrativo del departamento;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tienen los archivos de hojas de cálculo, hojas de texto y demás, en formatos digitales en cuentas asociadas al correo institucional.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

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

Fecha de actualización del documento de seguridad	16 de Octubre de 2024.

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**	Jesús josafat tirado fuentes
	Cargo	Jefe del Departamento de Planeación Estratégica
	Adscripción	Dirección de Planeación del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, características físicas, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, Clave Única de Registro de Población. **DATOS PERSONALES SENSIBLES.- Estado de salud física.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, 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 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		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 y 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 no se ha 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 puertametálica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. En el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento de Planeación Estratégica; Jefes de área del departamento; Estadígrafo del departamento; Auxiliar administrativo del departamento.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

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

Fecha de actualización del documento de seguridad	16 de Octubre de 2024.

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**	Alejandra Orozco Llamas
	Cargo	Director de Programas
	Adscripción	Dirección de Programas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones de la Responsable de Protección de Datos Personales del Sistema DIF Zapopan, actual Jefa de Departamento Titular 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** a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular 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 la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular 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		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

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

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

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta 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: • Director(a) de Programas; • Jefe del Departamento de la Delegación Institucional de la Procuraduría de Protección a Niñas, Niños y Adolescentes; • Jefe del Departamento de Protección a la Niñez y Adolescencia; • Jefe del Departamento de Paz • Jefe de Área B adscrita la Dirección de Programas • Unidad de Atención a Victimas de Violencia • Secretaria de Jefe de Departamento adscrita la Dirección de Programas
Procedimientos de respaldo y recuperación de datos personales	Además del archivo físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia.
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo

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

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

Fecha de actualización del documento de seguridad	22 de Octubre del 2024

Departamento de Paz y Habilidades Comunitarias

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**	Juan Jose Perez Pimentel
	Cargo	Encargado del Despacho del Departamento de Paz
	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 de la Responsable de Protección de Datos Personales del Sistema DIF Zapopan, actual Jefa de Departamento Titular 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** a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular 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 la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular 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 archiveros, con llave, así como en archivos digitales en la nube (plataforma drive), disco duro de la(s) computadora(s) asignada(s) que cuentan con una clave de usuario, a lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

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

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de 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: • JEFE DE DEPARTAMENTO • JEFES DE AREA A • JEFE DE ÁREA C • PSICOLOGAS/OS • SECRETARIAS • AUXILIARES ADMINISTRATIVOS DEL DEPARTAMENTO • AUXILIAR DE CENTRO • CONSEJEROS FAMILIARES • TRABAJADORES SOCIALES • SUPERVISORES DE PROGRAMA • EDUCADOR(A) • ADMINISTRADOR(A) DE DEPARTAMENTO • AUXILIAR GENERAL DE DEPARTAMENTO • ODONTÓLOGA (O) • PROMOTORES INFANTILES COMUNITARIOS
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia

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

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

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

Fecha de actualización del documento de seguridad	22 de Octubre del 2024

Departamento de Protección a la Niñez y Adolescencia

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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**	Marisol Briz Castillo
	Cargo	Jefe del Departamento de Protección a la Niñez y Adolescencia
	Adscripción	Dirección de Programas del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones de la Responsable de Protección de Datos Personales del Sistema DIF Zapopan, actual Jefa de Departamento Titular 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** a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular 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 la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular 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		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

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

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

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de 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: • JEFE DE DEPARTAMENTO • AUXILIAR ADMINISTRATIVO DEL DEPARTAMENTO • SECRETARIAS DEL DEPARTAMENTO • JEFE DE AREA B DEL DEPARTAMENTO • JEFE DE AREA C DEL DEPARTAMENTO • PROMOTORES INFANTILES COMUNITARIOS • PSICOLOGOS/AS • TRABAJADORES SOCIALES • JEFE DE AREA A • PROMOTORES DEL DEPARTAMENTO
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

Plan de trabajo

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

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

Fecha de actualización del documento de seguridad	22 de Octubre del 2024

Gobierno de Zapopan | Ciudad de los niños Direccion de Servicios

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

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

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha 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: Jefe del Departamento; Secretarias del departamento; Auxiliares Administrativos;

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

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

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

Fecha de actualización del documento de seguridad	25 de octubre de 2024

Gobierno de Zapopan | Ciudad de los niños

Departamento de Autismo

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 Autismo
Respecto del administrador de éste	**Nombre**	Lic. Carlos Eduardo Núñez Contreras
	Cargo	Jefe del Departamento de Autismo
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, fecha y lugar de nacimiento, edad, sexo, nacionalidad, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Unica de Registro de Población, RFC, número credencial de elector u otra identificación, estado divil, fotografía, parentescos, familiares o dependientes económicos. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en la nube, 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, 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 metálico, con llave, asi como en archivos digitales en la nube y en el disco duro de la computadora asignada.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

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

Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento de Autismo; Auxiliares o secretarias del departamento; Educadoras del Departamento; Psicólogas del departamento ; Coordinadoras de Autismo. Trabajo social
Procedimientos de respaldo y recuperación de datos personales	Se tiene resguardado el padrón de usuarios en el disco duro de la computadora y copia en USB, mientras que el expediente del usuario únicamente se encuentra en físico.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento no se cuenta con programa para la supresión y borrado seguro de los datos personales.

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

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

Fecha de actualización del documento de seguridad	25 de octubre de 2024

Gobierno de Zapopan | Ciudad de los niños

Departamento de Salud y Bienestar

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 Salud y Bienestar
Respecto del administrador de éste	**Nombre**	Dra. Socorro María Guadalupe Pastrana Pérez
	Cargo	Coordinadora de Salud y Bienestar
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, fecha y lugar de nacimiento, edad, sexo, nacionalidad, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Unica de Registro de Población, RFC, número credencial de elector u otra identificación, estado divil, fotografía, parentescos, familiares o dependientes económicos. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, 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 la bodega compartida con Autismo, 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	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con una puerta y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otra puerta con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.

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

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

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

Fecha de actualización del documento de seguridad	25 de octubre de 2024

Gobierno de Zapopan | Ciudad de los niños

Departamento del Centro Metropolitano del Adulto Mayor

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DIF Zapopan

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento del Centro Metropolitano del Adulto Mayor
Respecto del administrador de éste	**Nombre**	María Guadalupe Díaz González
	Cargo	Jefa del Departamento del Centro Metropolitano del Adulto Mayor
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		Se limita al registro y emisión de documentos o servicios internos del Departamento
Inventario de los datos personales		DATOS PERSONALES.- María Guadalupe Díaz Gonzalez, 30 de octubre de 1967, Guadalajara Jalisco, 57 años, sexo femenino, nacionalidad mexicna, firma, Características físicas; 171 mts estatura, 61 kg de peso, complexión delgada, responsable, proactiva, con compromiso institucional, vida afectiva familiar, domicilio particular: Fuente Minorca 1140, Villa Fontana Residencial, Tlaquepaque Jalisco, número de teléfono particular 3313860060 (celular), correo electrónico particular: diazglez.gpe@gmail.com, casa habitación en pago, automovil sedan nissan march, preferencia sexual: heterosexual, Clave Unica de Registro de Población: DIGG671030MJCZND05, RFC: DIGG671030TT9, número credencial de elector: DZGNGD67103014M801, estado divil: soltera, fotografía, se hace cargo de su padre de 82 años. **DATOS PERSONALES SENSIBLES.- Raza mestiza, sin antecedentes médicos de importancia tanto física como mentalmente, religión católica,sin afiliación política,**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en el disco duro de la computadora asignada y en archivos virtuales en línea, 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 un archiveros y locker de madera, con llave, asi como en archivos digitales 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. Al igual que en archivos compartidos en línea
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policia que resguarda las Instalaciones. 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: Jefe del Departamento del Centro Metropolitano del Adulto Mayor; Supervisores del departamento; Secretarias del departamento; Auxiliares Administrativos; Trabajadores Sociales; Abogados del Departamento; Psicólogo del Departamento; Enfermera del Departamento; Odontólogas del Departamento; y Podólogo del Departamento. Gerontólogos del Departamento, Médico del Departamento, Fisioterapéuteas asignados al Departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene información capturada en una base de datos, en la plataforma de gestión de usuarios y en archivos compartidos en línea
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

Fecha de actualización del documento de seguridad	25 de ocubre de 2024

Gobierno de Zapopan | Ciudad de los niños

Coordinación de Autismo

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 Autismo
Respecto del administrador de éste	**Nombre**	Lic. Karina Elizabeth Gómez González
	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, fecha y lugar de nacimiento, edad, sexo, nacionalidad, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Unica de Registro de Población, RFC, número credencial de elector u otra identificación, estado divil, fotografía, parentescos, familiares o dependientes económicos. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable de la Coordinación
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, 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 diagnósticos físicos, se encuentran numerados y resguardados en una archivero de metal, 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	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha 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	Los usuarios que tratan información en esta Coordinación son: Coordinador 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
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

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

Fecha de actualización del documento de seguridad	25 de octubre de 2024

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

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha registrado al momento incidente alguno.

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

Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Area, Trabajadora Social, Psicologa, Médico General y secretaria.
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
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

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

Fecha de actualización del documento de seguridad	28 de Octubre del 2024

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**	Maria del Carmen Karina Soria Hernandez
	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 memorias de USB, disco duro de la computadora asignada y informacion resguarda en el drive, a los cuales solo tiene acceso el personal responsable en cada Centro de Desarrollo Infantil.
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	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar al Centro de Desarrolo Infantil 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 CDIS se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archiveros de madera con chapa, en donde se resguardan los expedientes.

Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Area, Trabajadora Social, Psicologa, Médico General y secretaria.
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
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

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

Fecha de actualización del documento de seguridad	28 de octubre del 2024

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. Erika Guadalupe Cruz Ayala
	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 memorias de USB, disco duro de la computadora asignada y informacion resguarda en el drive, a los cuales solo tiene acceso el personal responsable en cada Centro de Desarrollo Infantil.
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	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha registrado al momento incidente alguno.

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

Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Area, Trabajadora Social, Psicologa, Médico General y secretaria.
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
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

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

Fecha de actualización del documento de seguridad	28 de octubre del 2024

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. Rosaura Soto 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 memorias de USB, disco duro de la computadora asignada y informacion resguarda en el drive, a los cuales solo tiene acceso el personal responsable en cada Centro de Desarrollo Infantil.
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	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha registrado al momento incidente alguno.

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

Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Area, Trabajadora Social, Psicologa, Médico General y secretaria.
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
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

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

Fecha de actualización del documento de seguridad	28 de octubre del 2024

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. Jazmín Alejandra Márquez Enríquez
	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 memorias de USB, disco duro de la computadora asignada y informacion resguarda en el drive, a los cuales solo tiene acceso el personal responsable en cada Centro de Desarrollo Infantil.
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	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha registrado al momento incidente alguno.

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

Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Area, Trabajadora Social, Psicologa, Médico General y secretaria.
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
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

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

Fecha de actualización del documento de seguridad	28 de octubre del 2024

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. Graciela García Pérez
	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 memorias de USB, disco duro de la computadora asignada y informacion resguarda en el drive, a los cuales solo tiene acceso el personal responsable en cada Centro de Desarrollo Infantil.
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	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha registrado al momento incidente alguno.

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

Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Area, Trabajadora Social, Psicologa, Médico General y secretaria.
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
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

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

Fecha de actualización del documento de seguridad	28 de octubre del 2024

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. Natalia Eugenia Ruelas Mejía
	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 memorias de USB, disco duro de la computadora asignada y informacion resguarda en el drive, a los cuales solo tiene acceso el personal responsable en cada Centro de Desarrollo Infantil.
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	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha registrado al momento incidente alguno.

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

Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Coordinación son: Jefa de Area, Trabajadora Social, Psicologa, Médico General y secretaria.
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
Se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora a la Responsable de Protección de Datos Personales del Sistema DIF Zapopan (Jefa de Departamento Titular de la Unidad de Transparencia).

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

Fecha de actualización del documento de seguridad	28 de octubre del 2024

Gobierno de Zapopan | Ciudad de los niños

Departamento de Trabajo Social

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 Trabajo Social
Respecto del administrador de éste	**Nombre**	Lic. Yadira Noemi Perez Villa
	Cargo	Jefa del Departamento de Trabajo Social
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, edad, sexo, firma, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, patrimonio, Clave Unica de Registro de Población y lugar de nacimiento. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Nacionalidad, 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 expedientes en físico, en caja de archivo, 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 de los expedientes activos, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados, en cada espacio fisico de las Trabajadoras Sociales. Cada una de ellas cuenta en su espacio fisico con un archivero con llave, 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	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

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

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 expedeintes (Es importante aclarar, 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 9 cámaras para poder indentificar algún suceso.

Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Jefe del Departamento de Trabajo Social, Responsable de la Ventanilla Unica del departamento, Recepcion del departamento, Trabajadoras Sociales del Centro de Trabajo Social. Trabajadoras Sociales del departamento operativas en los CDC´S . Trabajadoras Sociales del departamento de guarderías. Trabajadora Sociales de Salud y bienestar y de autismo. Personal Administrativo que lleva contro de documentos de usuarios; Secretaria del departamento; Coordinadora de CDCS. Coordinadora de guarderías.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

Fecha de actualización del documento de seguridad	24 de octubre de 2024

Coordinacion de Nutición y Asistencia Alimetnaria

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Departamento de la Coord de Nutrición y Asistencia Alimentaria
Respecto del administrador de éste	**Nombre**	C. Cynthia Maricela Barrera Naranjo
	Cargo	Coordinador de Nutrición y Asistencia Alimentaria
	Adscripción	Dirección de Servicios del Sistema DIF Zapopan
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Zapopan; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Zapopan, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Zapopan, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		DATOS PERSONALES.- Nombre, fecha y lugar de nacimiento, edad, sexo, nacionalidad, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, preferencia sexual, Clave Unica de Registro de Población, RFC, número credencial de elector u otra identificación, estado divil, fotografía, parentescos, familiares o dependientes económicos. **DATOS PERSONALES SENSIBLES.- Origen racial o étnico, Estado de salud física y mental e historial médico, información genética, datos biométricos y preferencia sexual.**
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en memoria USB, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Departamento y en la plataformas de captura de DIF Jalisco y de DIF Zapopan
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 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	Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 y en los archiveros de cada centro de DIF, 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 no se ha 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 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 otra puerta con chapa de seguridad y en el interior de ella se tienen los archivero en donde se resguardan los expedientes.

Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en este Departamento son: Coordinadora del departamento; Jefes de área; Secretarias de la coordinación; trabajadores sociales de alimentaria. Auxiliares Administrativos;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

Fecha de actualización del documento de seguridad	24 de octubre de 2024

Gobierno de Zapopan | Ciudad de los niños

Departamento de Habilidades y Profecionalización

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

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

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha 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: Jefe del Departamento; Secretarias del departamento; Auxiliares Administrativos;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

Fecha de actualización del documento de seguridad	24 de octubre de 2024

Dirección Jurídica

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha registrado al momento incidente alguno.

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

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

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

Fecha de actualización del documento de seguridad	25 de octubre de 2024

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**	Lic. María Fernanda Canales Espinoza
	Cargo	Jefa 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		DATOS PERSONALES: Nombre, fecha y lugar de nacimiento, edad, sexo, firma, domicilio particular, nacionalidad, número de teléfono particular, correo electrónico particular, CURP, RFC, número de credencial de elector y/o documentos de identificación, estado civil, fotografía, cuentas bancarias, parentescos, familiares o dependientes económicos. DATOS PERSONALES SENSIBLES.- historial médico, información genética, afiliación sindical, grado académico, huellas digitales, preferencia sexual.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en 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, asi 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		Se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, número de expediente, fojas del expediente, motivo de acceso u operación a la Información, fecha y hora de acceso o de operación del documento, firma de quien accede u opera la información, fecha y hora de devolución de la información y observaciones. De igual forma, se cuenta con la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: nombre y firma del responsable de la investigación, cargo, área, datos vulnerados, tipo de vulneración, fecha en que ocurrió, acciones correctivas implementadas de forma inmediata y definitiva y observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 no se ha 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 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 con doble chapa de seguridad y en el interior de ella se tienen archiveros donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Titular de la Unidad de Transparencia; y Auxiliar del Departamento
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene,
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con el programa NITRO para la supresión y borrado seguro de los datos personales.

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

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

Fecha de actualización del documento de seguridad	25 de octubre de 2024