Tel: 3030 3800
01 800 3000 343
Av. Alcalde # 1220,
Colonia Miraflores, C.P. 44270,
Guadalajara, Jalisco, México.

ACTA DE LA SEGUNDA SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DE DEL SISTEMA PARA EL DESARROLLO INTEGRAL DE LA FAMILIA DEL ESTADO DE JALISCO Y SUS ÓRGANOS DESCONCENTRADOS, DE FECHA UNO DE FEBRERO DE DOS MIL DIECINUEVE.----------

Guadalajara, Jalisco, siendo las doce horas con cinco minutos del día uno de febrero del año dos mil diecinueve, en la Sala de Juntas de Dirección General del Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco, ubicada en Avenida Alcalde número mil doscientos veinte, Colonia Miraflores de esta Ciudad, de conformidad con los artículos 24 fracción V, 27 al 30 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, así como el numeral 10 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, del mismo modo el 30 y 32 del Reglamento Interno de la Unidad de Transparencia e Información Pública del Sistema para la el Desarrollo Integral de la Familia del Estado de Jalisco, se convocó a la **Lic. Ana Lilia Mosqueda González**, en su carácter de Directora General y Presidenta del Comité de Transparencia del Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco, al **Lic. José de Jesús Segura de León**, Titular de la Unidad de Transparencia y Secretario del Comité de Transparencia y al Mtro. **Iván Valdez Rojas**, como Titular del Órgano de Control Interno e Integrante del Comité de Transparencia.----------

Haciendo uso de la voz la **Lic. Ana Lilia Mosqueda González**, Presidenta del Comité, le pidió al Secretario, el **Lic. José de Jesús Segura de León**, tomara la asistencia de los miembros del comité, encontrándose presentes los tres miembros que integran el Comité de Transparencia, a lo que la Presidenta declaró de manera formal la existencia del **Quórum Legal** para poder sesionar, conforme a lo estipulado en el artículo 29 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, y el 31 del Reglamento Interno de la Unidad de Transparencia e Información Pública del Sistema para la el Desarrollo Integral de la Familia del Estado de Jalisco.----------

Acto seguido, la Presidente del Comité, pidió al Secretario dar lectura y poner a consideración para su aprobación el Proyecto de Orden del Día siguiente: ----------

Primer Punto.- Presentación y en su caso aprobación del Plan Anual de Trabajo de la Unidad y Comité de Transparencia.----------

Segundo Punto.- Presentación, discusión y en su caso aprobación del proyecto de documento de Seguridad del Sistema DIF Jalisco y sus Órganos Desconcentrados, así como de las bitácoras de acceso y operación cotidiana y de vulneraciones a la seguridad de los datos personales, para dar cumplimiento a lo establecido en los

Tel: 3030 3800
01 800 3000 343
Av. Alcalde # 1220,
Colonia Miraflores, C.P. 44270,
Guadalajara, Jalisco, México.

numerales 35 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.----------

Tercer Punto.- Clausura y Aprobación del Acta de la Sesión del Comité de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados.----------

Una vez que el Secretario del Comité dio a conocer el Proyecto Orden del Día, este se pone a consideración de los integrantes del Comité para su aprobación, mismos que después de una deliberación lo aprobaron por **unanimidad**.----------

Acto siguiente, la Presidenta del Comité, puso a la consideración de los integrantes del Comité, la anuencia de la lectura del documento que fue circulado previamente, lo anterior, para entrar directamente a su votación, por lo que el Secretario del Comité, tomó la votación de la dispensa a la lectura del documento, la cual fue aprobada por **unanimidad**, así que se procedió abordar el primer punto del Orden del Día: ----------

Primer Punto del Orden del Día, Presentación y en su caso aprobación del Plan Anual de Trabajo de la Unidad y Comité de Transparencia.----------

La Presidenta del Comité de Transparencia hace referencia que es necesario establecer las acciones a ejecutar por la Unidad y Comité de Transparencia durante el año dos mil diecinueve, es por lo que se pone a consideración el plan anual de trabajo al presente órgano colegiado a fin de que lo analicen y realicen las manifestaciones que consideren necesarios o en su caso lo aprueben: ----------

I. La Unidad de Transparencia, por conducto de su Titular, otorgara de forma permanente atención y asesoría al público en materia de transparencia y acceso a la información.---------

II. La Unidad de Transparencia, por conducto de su Titular, llevara a cabo las funciones de oficialía de partes tanto de la Unidad como del propio Comité.----------

III. La Unidad de Transparencia, por conducto de su Titular, recibirá en un horario de 09:00 a 15:00 horas las solicitudes de información pública, en homologación al sistema INFOMEX, y dará respuesta a dentro de los ochos días hábiles que la Ley de la materia prevé.----------

IV. La Unidad de Transparencia, por conducto de su Titular, administrara los portales del sujeto obligado (Sistema DIF Jalisco, Museo Trompo Mágico y CEPAVI), relativo a la información pública fundamental y realizara las gestiones acciones para actualizarlo mensualmente de forma oportuna.----------

V. La Unidad de Transparencia, por conducto de su Titular, revisara de forma permanente los formatos de la Plataforma Nacional de Transparencia, los formatos serán llenados y subidos por las áreas generadoras, de forma mensual a la Plataforma.----------

VI. La Unidad de Transparencia, por conducto de su Titular, llevara el registro y estadística

Tel: 3030 3800
01 800 3000 343
Av. Alcalde # 1220,
Colonia Miraflores, C.P. 44270,
Guadalajara, Jalisco, México.

de las solicitudes de información pública a través del Sistema de Solicitudes de Información Respondidas (SIRES).----------

VII. La Unidad de Transparencia, por conducto de su Titular, tramitara en tiempo y forma los recursos de revisión y las solicitudes de protección de información confidencial que sean interpuestos.----------

VIII. El Comité de Transparencia sesionara de manera ordinaria al menos cada cuatro meses del presente año y de manera extraordinaria, las veces que sean necesarias.----------

IX. El Comité de Transparencia recibirá las solicitudes de acceso, clasificación, rectificación, oposición, modificación, corrección, sustitución, cancelación o ampliación de datos de la información confidencial, en un horario de 09:00 a 15:00 horas las solicitudes de información pública, en homologación al sistema INFOMEX, y dará respuesta en un plazo de diez días después de su admisión.----------

De lo anterior, se preguntó si se quería hacer alguna intervenciones, al no haberlas se procedió a tomar la votación correspondiente, siendo aprobado por **unanimidad**, y se continuo con el desahogo del siguiente punto del Orden del Día.----------

Segundo Punto del Orden del Día, Presentación, discusión y en su caso aprobación del proyecto de documento de Seguridad del Sistema DIF Jalisco y sus Órganos Desconcentrados, así como de las bitácoras de acceso y operación cotidiana y de vulneraciones a la seguridad de los datos personales, para dar cumplimiento a lo establecido en los numerales 35 y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.----------

En este acto, la Presidenta del Comité, le solicito al Secretario del Comité que diera cuenta sobre este punto, a lo que el Secretario comento que en virtud a lo consagrado en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, los entes públicos deben establecer y mantener medidas para la protección de los datos personales, para protegerlos de cualquier daño, perdida, alteración, destrucción, acceso o tratamiento no autorizado, con la finalidad de garantizar su confidencialidad, razón por lo que se creó este proyecto de Documento de Seguridad del Sistema DIF Jalisco y sus Organismos Desconcentrados en conjunto con las bitácoras de acceso y operación cotidiana y de vulneración a la seguridad de los datos personales, el cual se pone a su consideración para su aprobación, al terminar la intervención del Secretario, en uso de la voz la Presidenta hizo la mención que por haberse circulado con antelación el Proyecto antes mencionado y en razón de haberse aprobado la dispensa de su lectura se entrara al estudio, al no haber tenido intervenciones, se procedió a la votación correspondiente, siendo aprobado el documento de seguridad con sus bitácoras por

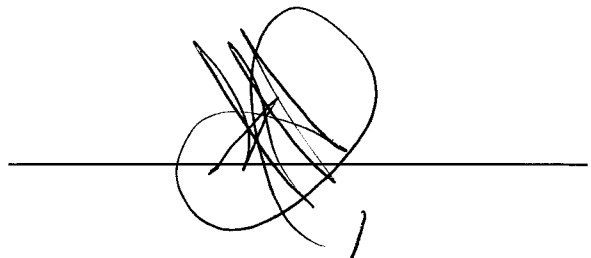
Tel: 3030 3800
01 800 3000 343
Av. Alcalde # 1220,
Colonia Miraflores, C.P. 44270,
Guadalajara, Jalisco, México.

unanimidad, continuando con el desahogo del tercer punto del Orden del Día.----------

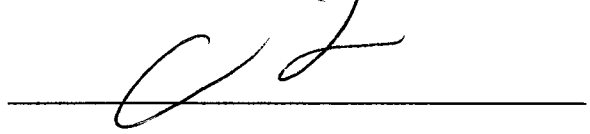
Tercer Punto del Orden del Día, Clausura y Aprobación del Acta de la Sesión del Comité de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados.----

A efecto de desahogar el último punto del Orden del Día y no haber tenido más asuntos por resolver, la Presidenta del Comité de Transparencia dio por clausurada la sesión del Comité de Transparencia, por lo que puso a consideración de los presente la aprobación del acta de la sesión, al no haber alguna observación, se procedió a la votación quedando aprobada por **unanimidad**, siendo las doce horas con treinta y tres minutos, del día uno de febrero del dos mil diecinueve, los integrantes del comité que intervinieron y quienes así quisieron hacerlo firmaron al margen y al calce, para los efectos legales a que haya lugar.----------

Lic. Ana Lilia Mosqueda González
Presidenta del Comité de Transparencia



Mtro. Iván Valdez Rojas
Titular del Órgano Interno de Control e
Integrante del Comité de Transparencia



Lic. José de Jesús Segura de León
Titular de la Unidad de Transparencia y
Secretario del Comité de Transparencia

Las firmas anteriores forman parte integral del acta de la sesión extraordinaria del día uno de febrero del dos mil diecinueve, del Comité de Trasparencia del Sistema para el Desarrollo Integral de la Familia en el Estado de Jalisco y sus Órganos Desconcentrados, misma que consta de cuatro fojas incluyendo la presente.- **CONSTE.----------**

BITACORA DE ACCESO Y OPERACIÓN COTIDIANA A LOS DATOS PERSONALES

Nombre del responsable de la información	Nombre de quien accede u opera la información	Motivo de acceso u operación a la información	Fecha y hora de acceso o de operación del documento	Firma de quien accede u opera la información	Fecha y hora de devolución de la información	Observaciones

BITACORA DE VULNERACIONES A LA SEGURIDAD DE LOS DATOS PERSONALES (Pérdida o destrucción no autorizada; robo, extravío o copia no autorizada; uso, acceso o tratamiento no autorizado; o el daño, la alteración o modificación no autorizada)

Fecha en que ocurrió	El motivo de la vulneración de seguridad	Acciones correctivas implementadas de forma inmediata y definitiva	El daño, la alteración o modificación no autorizada	Observaciones

Museo Trompo Mágico

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**	Marcela Gómez Ramírez
	Cargo	Directora del Museo Trompo Mágico
	Adscripción	Museo Trompo Mágico
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 Jalisco; • **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 Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.-** Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, correo electrónico particular, Clave Única de Registro de Población.
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 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 federales y/o 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 archiveros y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros del Museo Trompo Mágico, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar al edificio se cuenta con tres puertas metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Museo Trompo Mágico, se cuenta con otras puertas, con chapa de seguridad y en el interior de ella se tienen los archiveros donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el Museo Trompo Mágico son: • Marcela Gómez Ramírez, Museo Trompo Mágico;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

El Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		El Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar
Respecto del administrador de éste	**Nombre**	Eunice Adriana Avilés Valencia
	Cargo	Jefa de la Unidad Departamental de CEPAVI
	Adscripción	El Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar
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 Jalisco, actual 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** al Responsable de Protección de Datos Personales del Sistema DIF Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente, Autoridades del Sistema de Justicia, Fiscalía Estatal.
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 el disco duro de las computadoras asignadas, a la cual solo tiene acceso el personal responsable del Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar.
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 federales y/o 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 archivos digitales disco duro de las computadoras asignadas que cuentan con una clave de usuario, a lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

Análisis de riesgos

Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en estos Organismos, 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 los equipos de cómputo del Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar, para evitar que el personal no autorizado, tenga acceso a ellos; es que algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policia que resguarda las Instalaciones y una persona que controla ingresos a las mismas. Para ingresar al edificio 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 las oficinas del Consejo, se cuenta con otras puertas, 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 el Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar: • Eunice Adriana Avilés Valencia, Jefa de la Unidad Departamental de CEPAVI; • Aurora de la Mora Mendez, Licenciatura de Trabajo Social de CEPAVI;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Unidad de Transparencia
Respecto del administrador de éste	**Nombre**	José de Jesús Segura de León
	Cargo	Titular de la Unidad de de Transparencia
	Adscripción	Dirección Jurídica
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 Jalisco; • **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 Jalisco, 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 Jalisco, 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.
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 Unidad de Transparencia.
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 archiveros con llave, así como en archivos digitales en memoria USB y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que 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 Dirección, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay elementos de policía custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones

Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas son tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además para ingresar a las oficinas de la Unidad de Transparencia, se cuenta con puertas de madera, con chapa de seguridad y en el interior de ella se tienen archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Unidad de Transparencia son: • José de Jesús Segura de León, Titular de la Unidad de Transparencia; • Maria de Lourdes Gomez Carillo, Jefe de Sección B; • Alejandra Montserrat Garcia Olivares, Licenciatura;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Procuraduría de Protección a Niñas, Niños y Adolescentes

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Procuraduría de Protección a Niñas, Niños y Adolescentes
Respecto del administrador de éste	**Nombre**	Alejandra Salas Niño
	Cargo	Procuradura de Protección de Niñas, Niños y Adolescentes del Estado de Jalisco
	Adscripción	Procuraduría de Protección de Niñas, Niños y Adolescentes del Estado de Jalisco
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 Jalisco, actual 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** al Responsable de Protección de Datos Personales del Sistema DIF Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente, Autoridades del Sistema de Justicia, Fiscalía Estatal.
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 el disco duro de las computadoras asignadas, a la cual solo tiene acceso el personal responsable de la Procuraduría de Protección de Niñas, Niños y Adolescentes.
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 federales y/o 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 archiveros con llave, así como en archivos digitales disco duro de las computadoras asignadas con que se cuentan, teniendo una clave de usuario, a lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

Análisis de riesgos

Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en estos Organismos, 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 Procuraduria de Protección de Niñas, Niños, para evitar que personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay un control de acceso a las intalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policia que resguarda las Instalaciones y una persona que controla ingresos a las mismas. Para ingresar al edificio 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 las oficinas de la Procuraduria de Protección de Niñas, Niños y Adolescentes, se cuenta con otras puertas, 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 la Procuraduría de Protección de Niñas, Niños y Adolescentes: • Alejandra Salas Niño, Procuradora de Protección de Niñas, Niños y Adolescentes; • Norma de Jesús Villafaña Preciado, Directora de Prevención; • Rosa del Carmen Ochoa Cota, Directora de Atención y Protección; • Luis Antonio Gómez Hurtado, Director de Representación y Restitución; • María Raquel Arias Covarrubias; Directora de Tutela de Derechos;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco (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 Jalisco (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	30 de Enero de 2019

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**	Luis Alberto Castro Rosales
	Cargo	Director Jurídico
	Adscripción	Dirección Jurídica
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 Jalisco; • **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 Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.** Nombre, edad, sexo, firma, Características físicas, morales, domicilio particular, número de teléfono particular, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.** Historial médico, 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 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 federales y/o 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 archiveros con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitácora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con tres puerta metalicas 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 archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Dirección son: • Luis Alberto Castro Rosales, Director Jurídico; • Diego Armando Calixto Guzmán, Jefe de Departamento de Control de Siniestros y Bienes Inmuebles; • Jorge Alberto Reséndiz Flores, Jefe de Unidad Departamental de Asuntos Laborales; • Francisco Alonso Moreno Muñoz, Jefe de Departamento de Acuerdos y Asuntos Jurídicos;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Contraloría Interna (Órgano Interno de Control)

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Contraloría Interna
Respecto del administrador de éste	**Nombre**	Iván Valdez Rojas
	Cargo	Contralor Interno (Titular del Órgano Interno de Control)
	Adscripción	Contraloría del Sistema DIF Jalisco (Órgano Interno de Control)
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 Jalisco; • **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 Jalisco, 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 Jalisco, 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. 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 Interna.
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 federales y/o 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 archiveros, con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la Información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros de la Contraloría Interna, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa; hay elementos de policía custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones

Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitácora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas 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 puertas metalicas y con cristal 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 la Contraloría Interna son: • Iván Valdez Rojas, Contralor Interno (Titular del Órgano Interno de Control); • Alondra Dolores Vidrio Mendoza, Responsabilidades Administrativas; • Juana Elizabeth Guzmán Elías, Auditorias;
Procedimientos de respaldo y recuperación de datos personales	Se cuenta en expediente físico.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección de Recursos Humanos

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales dela Dirección de Recursos Humanos
Respecto del administrador de éste	**Nombre**	María del Rosario Salinas Villalobos
	Cargo	Directora de Recursos Humanos
	Adscripción	Dirección de Recursos Humanos
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 Jalisco; • **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 Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.**- Nombre, edad, sexo, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.**- Origen racial o étnico, Estado de salud física y mental e historial médico, datos biométricos, afiliación sindical, creencias religiosas, filosóficas y morales, opiniones políticas.
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 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 federales y/o 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 archiveros 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		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros del Dirección, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay elementos de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas son tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina dela Dirección, se cuenta con puertas de madera y metal, 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 la Dirección de Recursos Humanos son: • María del Rosario Salinas Villalobos, Directora de Recursos Humanos; • Aurora Carolina González Hidalgo, Administración De Personal; • Yuriria Jazmín Tonanzing Ríos Gutiérrez, Desarrollo de Personal y Servicio Social; • Yesika Nayeli Gutiérrez Jiménez, Prestaciones y Servicios;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección de Recursos Financieros

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Recursos Financieros
Respecto del administrador de éste	**Nombre**	Ana Elena González Jaime
	Cargo	Directora de Recursos Financieros
	Adscripción	Dirección 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 Jalisco; • **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 Jalisco, 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 Jalisco, 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.
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 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 federales y/o 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 archiveros 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		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros de la Dirección, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay elementos de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas 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 otras puertas de metalicas con cristal, 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 la Dirección de Recursos Financieros son: • Ana Elena González Jaime, Directora de Recursos Financieros; • Jorge Ulises Segura Domínguez, Presupuestos; • Luz Angélica López Ortiz, Contabilidad; • Gildardo Mendoza Juárez, Tesorería;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección de Recursos Materiales

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Recursos Materiales
Respecto del administrador de éste	**Nombre**	Iván Alejandro Bravo Reza
	Cargo	Director de Recursos Materiales
	Adscripción	Dirección de Recursos Materiales
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 Jalisco; • **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 Jalisco, 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 Jalisco, 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.
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 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 federales y/o 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 archiveros 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		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros de la Dirección de Recursos Materiales, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay elementos de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.
Gestión de vulneraciones

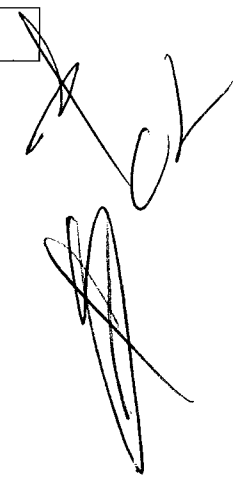
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas 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 otras puertas de metalicas con cristal, con chapa de seguridad y en el interior de ella se tienen los archiveros donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Recursos Materiales son: • Iván Alejandro Bravo Reza, Director de Recursos Materiales; • Alberto Clemente Preciado García, Activos Fijos; • Esther Fausto Brito, Almacén; • Roberto Alejandro Valladares Zamudio, Compras;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019



Dirección de Planeación

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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**	Ernesto Jesús Ivon Pliego
	Cargo	Director de Planeación
	Adscripción	Dirección de Planeación
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 Jalisco; • **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 Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.-** Nombre, edad, sexo, firma, características físicas, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, Clave Única de Registro de Población.
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 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 federales y/o 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 el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en los equipos de cómputo de la Dirección, para evitar que el personal no autorizado, tenga acceso a ellos; es que algunos equipos de cómputo cuenta con contraseñas alfanuméricas, aunque carecen 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 oficiales de policía que resguarda las Instalaciones y controla ingresos a las mismas.Para ingresar a las oficinas cuenta con tres puerta metalicas 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 otras puertas de madera, con chapa de seguridad.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Planeación son: • Ernesto Jesús Ivon Pliego, Director de Planeación; • Héctor Juárez Ayard; Planeación; • Karen Lizette Abreu Rodríguez, Evaluación; • Alejandra Romo Arias, Profesionalización; • Laura Olivia Delgado Avila, Desarrollo Institucional;
Procedimientos de respaldo y recuperación de datos personales	Los archivos se encuentra 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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad	Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección de Servicios Generales

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Dirección de Servicios Generales
Respecto del administrador de éste	**Nombre**	Martín Rubén Corona González
	Cargo	Director de Servicios Generales
	Adscripción	Dirección de Servicios Generales
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 Jalisco; • **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 Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.**- Nombre, edad, sexo, firma, vida afectiva familiar, domicilio particular. **DATOS PERSONALES SENSIBLES.**- datos biométricos.
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 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 federales y/o 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 archiveros con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas 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 archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Servicios Generales son: • Martín Rubén Corona González, Director de Servicios Generales; • Luis Rosendo Rodriguez Peña, Protección Civil DIF Jalisco;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección de Trabajo Social y Vinculación

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Dirección de Trabajo Social y Vinculanción
Respecto del administrador de éste	**Nombre**	María Eugenia Gutiérrez Solís
	Cargo	Directora de Trabajo Social y Vinculanción
	Adscripción	Dirección de Trabajo Social y Vinculación
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 Jalisco; • **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 Jalisco, 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 Jalisco, 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 morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, patrimonio, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.-** Origen racial o étnico, Nacionalidad, lugar de nacimiento, datos biométricos, teléfono particular y uno adicional donde dejar recados, Integrantes de la familia, ingreso familiar mensual, servicios médicos, y familiares con enfermedades crónicas o discapacidad.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable de la Dirección, 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 federales y/o 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 archiveros 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		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas). Existe el gran riesgo de que los expedientes se encuentren bajo su resguardo, ya que en ocaciones que no acuden a laborar y los ususarios se presentan, por lo que sera necesario trasladarlos a un area comun, para mejor control y seguimiento.

Análisis de brecha

Los expedientes se encuentran en archiveros de la Dirección, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay elementos de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas 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 otras puertas de metalicas con cristal, 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 la Dirección de Trabajo Social y Vinculación son: • María Eugenia Gutiérrez Solís, Directora de Trabajo Social y Vinculación; • Ma Soveida Martinez Campos, Trabajo Social Operativo;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección para el Desarrollo Integral del Adulto Mayor

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Dirección para el Desarrollo Integral del Adulto Mayor
Respecto del administrador de éste	**Nombre**	María Asensión Álvarez Solís
	Cargo	Directora para el Desarrollo Integral del Adulto Mayor
	Adscripción	Dirección para el Desarrollo Integral del Adulto Mayor
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 Jalisco; • **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 Jalisco, 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 Jalisco, 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 fica, morales o emocionalesvida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, Clave Única de Registro de Población. **DATOS PERSONALES SENSIBLES.-** Lugar de procedencia, Estado de salud física y mental e historial médico, datos biométricos, Integrantes de la familia.
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 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 federales y/o 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 archiveros 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		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros de la Dirección, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay elementos de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones

Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas 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 otras puertas de metalicas con cristal, 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 la Dirección para el Desarrollo Integral del Adulto Mayor son: • María Asensión Álvarez Solís, Directora para el Desarrollo Integral del Adulto Mayor; • Yarib Michael Limón Villa, Vinculación; • Angelica Contreras Robles, Centros de Día;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección de Atención a la Primera Infancia

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Atención a la Primera Infancia
Respecto del administrador de éste	**Nombre**	José Martín Díaz de León Díaz de León
	Cargo	Director de Atención a la Primera Infancia
	Adscripción	Dirección de Atención a la Primera Infancia
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 Jalisco; • **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 Jalisco, 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 Jalisco, 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 y emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, estado civil, Clave Única de Registro de Población (CURP), Registro Federal de Contribuyentes. DATOS PERSONALES SENSIBLES. Nacionalidad, estado de salud física y mental, historial médico, información genética, creencias religiosas, filosóficas y morales.
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 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 federales y/o 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 archiveros, con llave, así como en archivos digitales disco duro de la(s) computadora(s) asignada(s) que cuentan con una clave de usuario, a lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitácora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas 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 otras puertas de metalicas con cristal, 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 la Dirección de Atención a la Primera Infancia son: • José Martín Díaz de León Díaz de León, Director de Atención a la Primera Infancia; • Angelina Tereshkova Juarez Ayard, Estrategia para Lactantes, Maternales y Preescolares; • Tania Yahaira Ramirez De La Rocha, Dirección de Atención a la Primera Infancia;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará, por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad	Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección para la Inclusión de las Personas con Discapacidad

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección para la Inclusión de las Personas con Discapacidad
Respecto del administrador de éste	**Nombre**	María Itzel Parada Lupercio
	Cargo	Directora de la Inclusión de las Personas con Discapacidad
	Adscripción	Dirección para la Inclusión de las Personas con Discapacidad
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 Jalisco; • **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 Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.-** Nombre, edad, sexo, fecha de nacimiento, nombre de los tutores, vida afectiva familiar, vida escolar, domicilio particular, número de teléfono particular, correo electrónico particular. **DATOS PERSONALES SENSIBLES.-** Diagnóstico médico, Estado de salud física y mental, historial médico, estudios neurológicos, evaluación de desarrollo de habilidades, reporte de avances terapéuticos
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos digitales en el disco duro de la computadora signada, a la cual tiene acceso el responsable de la Dirección 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 federales y/o 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 archiveros, con llave, asi como en archivos digitales en el disco duro de la computadora asignada.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros de la Dirección, para evitar que el personal 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 guardia de seguridad privada que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con una puerta metalica y cristal con 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 otras puertas 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 la Dirección para la Inclusión de las Personas con Discapacidad son: • María Itzel Parada Lupercio, Dirección para la Inclusión de las Personas con Discapacidad; • Stephanie Santos, Desarrollo de Habilidades para la Vida; • Miriam Alejandra Vazquez Casillas, Centro de Atención Cien Corazones; • Liliana Arcelia Gutierrez Gomez, Clínica de Atención Especial;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección de Seguridad Alimentaria

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Seguridad Alimentaria
Respecto del administrador de éste	**Nombre**	Marcela Guadalupe Aceves Sánchez
	Cargo	Directora de Seguridad Alimentaria
	Adscripción	Dirección de Seguridad Alimentaria
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 Jalisco; • **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 Jalisco, 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 Jalisco, 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. **DATOS PERSONALES SENSIBLES.-** Datos generales de su domicilio con cruces y colonia, así como municipio de nacimiento, Integrantes de la familia, ingreso familiar mensual.
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 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 archiveros 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		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros de la Dirección, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay elementos de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas 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 otras puertas de metalicas con cristal, 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 la Dirección de Seguridad Alimentaria son: • Marcela Guadalupe Aceves Sánchez, Directora de Seguridad Alimentaria; • Alejandra Maytorena Sandoval, Nutrición Escolar; • Karen Joanna Lizbeth Patiño Hurtado, Orientación Alimentaria;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección de Desarrollo Comunitario y Apoyo Municipal

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Desarrollo Comunitario y Apoyo Municipal
Respecto del administrador de éste	**Nombre**	Israel González Ramírez
	Cargo	Subdirector General de Fortalecimiento Municipal
	Adscripción	Subdirección General de Fortalecimiento Municipal
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 Jalisco; • **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 Jalisco, 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 Jalisco, 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, Clave Única de Registro de Población (CURP), datos biométricos.
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 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 federales y/o 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 archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como 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 no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay elementos 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 oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas 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 otras puertas de metalicas con cristal, 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 la Dirección de Desarrollo Comunitario y Apoyo Municipal son: • Israel González Ramírez, Subdirector General de Fortalecimiento Municipal; • Teresa Luna Palafox, Vinculación Municipal; • Yadira Larios Preciado, Región 02 Altos Norte; • Anna Elizabeth Ramirez Mares, Zona Centro; • Alba Rosa Azpeitia Sanchez, Zona Sur;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección de Relaciones Públicas

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Relaciones Públicas
Respecto del administrador de éste	**Nombre**	Pedro Pablo López Martínez
	Cargo	Director de Relaciones Públicas
	Adscripción	Dirección de Relaciones Públicas
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 Jalisco; • **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 Jalisco, 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 Jalisco, 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, domicilio particular, número de teléfono particular, correo electrónico particular, Clave Única de Registro de Población, Registro Federal de Contribuyentes.
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 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 federales y/o 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 archiveros 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		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha

Los expedientes se encuentran en archiveros de la Dirección, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay elementos de policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas 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 otras puertas de metalicas con cristal, 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 la Dirección de Recursos Financieros son: • Pedro Pablo López Martínez, Director de Relaciones Públicas;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Dirección de Tecnologías y Sistemas de Información

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Tecnologías y Sistemas de Información
Respecto del administrador de éste	**Nombre**	Jorge Chavez Ruiz
	Cargo	Jefe del Departamento de Infraestructura Tecnológica
	Adscripción	Dirección de Tecnologías y Sistemas de Información
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 Jalisco; • **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 Jalisco, 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 Jalisco, 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. **DATOS PERSONALES SENSIBLES.**- Datos generales de su domicilio con cruces y colonia, así como municipio de nacimiento, Integrantes de la familia, ingreso familiar mensual.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en el Servidor del Organismo, la cual solo tiene acceso el personal responsable.
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 en archivos digitales en el Servidor del Organismo, a todo lo cual solo tiene acceso el personal responsable.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los archivos se encuentran en en el Servidor del Organismo, para evitar que el personal no autorizado, tenga acceso a ellos, este se encuentra en un lugar aislado y cerrado; hay elementos de policia custodiando instalaciones.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas 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 otras puertas de metalicas con cristal, con chapa de seguridad.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Tecnologías y Sistemas de Información son: • Jorge Chavez Ruiz, Jefe del Departamento de Infraestructura Tecnológica;
Procedimientos de respaldo y recuperación de datos personales	Se tiene resguardada la información en el Servidor del Organismo.
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Luz Elena Perez Guzmán
	Cargo	Jefe de departamento del C.A.D.I. 2
	Adscripción	
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 Jalisco; • **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 Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.-** Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.-** Estado de salud física y emocional e historial médico.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en archiveros con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades federals y/o 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 archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, algunos equipos de computo carecen de contraseña alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	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, ademas con un filtro para el ingreso, ademas se cuenta con un guardia de seguridad privada que resguarda las instalaciones, para ingresar a las oficinas de los Centros de Atención, se cuenta con puertas con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el C.A.D.I. 02 son: • Luz Elena Perez Guzmán, Jefa del Departamento de C.A.D.I. 02;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Marisela Perez Garcia
	Cargo	Jefe de departamento del C.A.D.I. 6
	Adscripción	Centro Asistencial de Desarrollo Infantil numero 06
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 Jalisco; • **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 Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.-** Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.-** Estado de salud física y emocional e historial médico.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en archiveros con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades federals y/o 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 archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, algunos equipos de computo carecen de contraseña alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	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, ademas con un filtro para el ingreso, ademas se cuenta con un guardia de seguridad privada que resgurda las instalaciones, para ingresar a las oficinas de los Centros de Atención, se cuenta con puertas con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el C.A.D.I. 06 son: • Marisela Perez Garcia, Jefa del Departamento de C.A.D.I. 06;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Ruth Cisneros Martin
	Cargo	Jefe de departamento del C.A.D.I. 7
	Adscripción	Centro Asistencial de Desarrollo Infantil numero 07
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 Jalisco; • **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 Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.-** Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.-** Estado de salud física y emocional e historial médico.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en archiveros con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades federals y/o 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 archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, algunos equipos de computo carecen de contraseña alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	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, ademas con un filtro para el ingreso, ademas se cuenta con un guardia de seguridad privada que resgurda las instalaciones, para ingresar a las oficinas de los Centros de Atención, se cuenta con puertas con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el C.A.D.I. 07 son: • Ruth Cisneros Martin, Jefa del Departamento de C.A.D.I. 07;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Susana Fonseca Madrigal
	Cargo	Jefe de departamento del C.A.D.I. 8
	Adscripción	Centro Asistencial de Desarrollo Infantil numero 08
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 Jalisco; • **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 Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.-** Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.-** Estado de salud física y emocional e historial médico.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en archiveros con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades federals y/o 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 archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, algunos equipos de computo carecen de contraseña alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	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, ademas con un filtro para el ingreso, ademas se cuenta con un guardia de seguridad privada que resgurda las instalaciones, para ingresar a las oficinas de los Centros de Atención, se cuenta con puertas con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el C.A.D.I. 08 son: • Susana Fonseca Madrigal, Jefa del Departamento de C.A.D.I. 08;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Coordinación de Centros de Atención
Respecto del administrador de éste	**Nombre**	Karen Alicia Mata Ornelas
	Cargo	Jefe de departamento del C.A.D.I. 10
	Adscripción	Centro Asistencial de Desarrollo Infantil numero 10
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 Jalisco; • **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 Jalisco, 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 Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**DATOS PERSONALES.-** Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, patrimonio, ingresos económicos, correo electrónico particular, Ocupación, Escolaridad, Clave Única de Registro de Población, Registro Federal de Contribuyentes. **DATOS PERSONALES SENSIBLES.-** Estado de salud física y emocional e historial médico.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales		Se tiene la información resguardada en archivos físicos en archiveros con llave y digitales en el disco duro de la computadora asignada, a los cuales solo tiene acceso el personal responsable en cada Centro de Atención.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen		La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades federals y/o 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 archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales		A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros de cada Centro de Atención, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, algunos equipos de computo carecen de contraseña alfanumericas de alta seguridad.

Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	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, ademas con un filtro para el ingreso, ademas se cuenta con un policia que resgurda las instalaciones, para ingresar a las oficinas de los Centros de Atención, se cuenta con puertas con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el C.A.D.I. 10 son: • Karen Alicia Mata Ornelas, Jefa del Departamento de C.A.D.I. 10;
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 la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, 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	30 de Enero de 2019