Tel. 3030 9800
01 800 2000 543
Av. Alcalde # 1220,
Colonia Miraflores C.P. 44270,
Guadalajara, Jalisco, México

ACTA DE LA VIGÉSIMA QUINTA SESIÓN EXTRAORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL SISTEMA PARA EL DESARROLLO INTEGRAL DE LA FAMILIA DEL ESTADO DE JALISCO Y SUS ÓRGANOS DESCONCENTRADOS, DE FECHA SIETE DE NOVIEMBRE DE DOS MIL DIECINUEVE.----------

Guadalajara, Jalisco, siendo las trece horas con dos minutos del día siete de noviembre 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 15 al 19 del Reglamento Interno de la Unidad de Transparencia del Sistema para el Desarrollo Integral de la Familia de Jalisco, se convocó al **Ing. Juan Carlos Martin Mancilla**, en su carácter de Director General y Presidente 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 a la **Lic. Juana Elizabeth Guzman Elias**, como Titular del Órgano Interno de Control e Integrante del Comité de Transparencia, también se encontró presente con voz pero sin voto, el **Mtro. Luis Alberto Castro Rosales**, Director Jurídico del Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco.----------

Ing. Juan Carlos Martin Mancilla, Presidente del Comité de Transparencia: Buenas tardes, agradezco la presencia de todos ustedes, conforme a lo establecido en Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y el Reglamento Interno de la Unidad de Transparencia del Sistema para el Desarrollo Integral de la Familia de Jalisco, siendo las trece horas con dos minutos del día siete de noviembre de dos mil diecinueve, vamos a dar inicio a la vigésima quinta sesión con carácter de extraordinaria de este Comité de Transparencia del Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco y sus Órganos Desconcentrados, por lo que le pido al Secretario tome la asistencia y verifique la existencia del quórum legal necesario para esta sesión.----------

Lic. José de Jesús Segura de León, Secretario del Comité de Transparencia: En seguida Presidente, buenas tardes a todos, para efectos de esta sesión hago constar que se encuentran presentes tres miembros del Comité de Transparencia de este

[redacted]
Av. [redacted]
Colonia Miraflores, C.P. 44270,
Guadalajara Jalisco, México

Sujeto Obligado, por lo que existe el quórum para su realización. También informo que concurre a la presente sesión con voz pero sin voto, el **Mtro. Luis Alberto Castro Rosales**, Director Jurídico del Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco.----------

Presidente del Comité: En vista de lo anterior, **declaró formalmente instalada** la Vigésima Cuarta Sesión del Comité de Transparencia, misma que tiene el carácter de extraordinaria, por lo que pido al Secretario dar lectura al orden día que tenemos para esta sesión.----------

Secretario del Consejo: En seguida, el proyecto de orden del día que se somete a su consideración es el siguiente:----------

Primer Punto.- Proyecto de actualización del documento de Seguridad del Sistema para el Desarrollo Integral de la Familia de Jalisco, 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.----------

Segundo Punto.- Proyecto de actualización de los Avisos de Privacidad del Sistema DIF Jalisco y sus Órganos Desconcentrados.----------

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

Es todo Presidente.----------

Presidente del Comité: Gracias Secretario, está a su consideración de los presentes el proyecto del orden del día. Si no hay intervenciones le pido Secretario que consulte si se aprueba el mismo.----------

Secretario del Comité: Integrantes del Comité, se consulta si se aprueba el orden del día, los que estén por la afirmativa levanten la mano. Quedó aprobado por **unanimidad** el orden del día.----------

Presidente del Comité: Muchas gracias Secretario inicie el desahogo del orden del día.----------

Secretario del Comité: El **Primer punto** del orden del día, corresponde **Proyecto de actualización del documento de Seguridad del Sistema para el Desarrollo Integral de la Familia de Jalisco, 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**

Tel. 3030 3900
01 800 5000 343
Av. Alcalde # 1270
Colonia Miraflores CP 44270
Guadalajara, Jalisco, México

de Datos Personales en Posesión de Sujetos Obligados.----------

Presidente del Comité: Integrantes del Comité, está a la consideración de ustedes el Proyecto de actualización del documento de Seguridad del Sistema para el Desarrollo Integral de la Familia de Jalisco, lo anterior con la finalidad de tenerlo actualizado, cumpliendo así con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados. Si no hay ninguna intervención, señor Secretario le pido por favor que tome la votación correspondiente.----------

Secretario del Comité: Claro que sí, se consulta si se aprueba el proyecto de Documento de Seguridad, quienes estén por la afirmativa, levanten la mano por favor, quedo aprobado por **unanimidad** el Documento de Seguridad.----------

Presidente del Comité: Gracias Secretario continúe con el desahogo del orden del día.----------

Secretario del Comité: El **Segundo Punto** del Orden del Día corresponde en el **Proyecto de actualización de los Avisos de Privacidad del Sistema DIF Jalisco y sus Órganos Desconcentrados.**----------

Presidente del Comité: Integrantes del Comité, está a la consideración de ustedes los Proyectos de los Avisos de Privacidad del Sistema DIF Jalisco y sus Órganos Desconcentrados, de acuerdo con el documento de seguridad previamente aprobado. Si no hay ninguna intervención, señor Secretario le pido por favor que tome la votación correspondiente.----------

Secretario del Comité: Claro que sí, se consulta si se aprueba los proyectos de Avisos de Privacidad, quienes estén por la afirmativa, levanten la mano por favor, quedo aprobado por **unanimidad**.----------

Presidente del Comité: Gracias Secretario continúe con el desahogo del orden del día.----------

Secretario del Comité: el **Tercer Punto** del Orden del Día corresponde **en la Clausura y Aprobación del Acta de la Sesión del Comité de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados**.----------

Presidente del Comité: Al no haber más puntos por resolver, procedo a dar por clausurada la sesión del Comité de Transparencia, por lo que pongo a su consideración la aprobación del acta de esta sesión. Si no hay intervención alguna, Secretario le pido que tome la votación correspondiente.----------

Secretario del Comité: Integrantes del Comité se consulta si se aprueba el acta de la presente sesión, quienes estén por la afirmativa, levanten la mano por favor, quedo

Tel. 3030 3580
01 800 3600 348
Av. Alcalde # 950,
Colonia Miraflores, C.P. 44270,
Guadalajara, Jalisco, México.

aprobado por **unanimidad.**----------

Presidente del Comité: Gracias Secretario, agradezco a todos su presencia a esta sesión, siendo las trece horas con veinte minutos del día siete de noviembre del dos mil diecinueve, se da por concluida la vigésima quinta sesión extraordinaria del Comité de Transparencia.----------

Se levanta la presente acta que consta de cuatro fojas útiles por su lado anverso y sus anexos, firmando al margen y calce para constancia legal por los integrantes del Comité de Transparencia, para los efectos legales a que haya lugar. ----------

Ing. Juan Carlos Martin Mancilla
Presidente del Comité de Transparencia

Lic. Juana Elizabeth Guzman Elias
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

Mtro. Luis Alberto Castro Rosales
Director Jurídico del Sistema DIF Jalisco

Las firmas anteriores forman parte integral del acta de la sesión extraordinaria del día siete de noviembre 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. **CONSTE.**----------

Museo Trompo Mágico

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Mueso Trompo Mágico
Respecto del administrador de éste	**Nombre**	Marcela Gómez Ramírez
	Cargo	Directora del Museo Trompo Mágico
	Adscripción	Dirección General 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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Museo Trompo Mágico

FICHA DE PROTECCIÓN DE DATDS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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 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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros 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

Museo Trompo Mágico

FICHA DE PRDTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del Museo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Pnsesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar

FICHA DE PROTECCIÓN DE DATDS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de Datos Personales del Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar
Respecto del administrador de éste	**Nombre**	Eunice Adriana Avilés Valencia
	Cargo	Directora del Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar
	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).
		Nivel de Seguridad Básica: • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Niveles de Seguridad de los Datos Personales	**Nivel de Seguridad Media:** • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, 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 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.

Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar

FICHA OE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD

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

- Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos;
- El personal del Consejo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco.
- Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares.
- Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales.
- En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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, directora del CEPAVI; • Aurora de la Mora Mendez, Licenciatura de Trabajo Social de CEPAVI; • Alejandra Salas Niño, Procuradora de Protección de Niñas, Niños y Adolescentes;
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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.

Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD

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		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados

FICHA DE PROTECCIÓN DE OATOS 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	Jefe de Departamento 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 Pratección 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.
Niveles de Seguridad de los Datos Personales		Nivel de Seguridad Básica: • Datos de identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • Datos laborales: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros
		Nivel de Seguridad Media: • Datos patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • Datos sobre procedimientos administrativos seguidas en forma de juicio y/o procesos jurisdiccionales: Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, can independencia de su etapa de trámite • Datas académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • Datos de tránsita y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados

FICHA DE PROTECCIÓN DE OATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que 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

Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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, Jefe de Departamento 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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes qoe deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Fecha de actualización del documento de seguridad	Noviembre del 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	Luis Antonio Gómez Hurtado
	Cargo	Procurador 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 jurídicos.
		Nivel de Seguridad Básica: • **Datos de identificación**: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales**: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

Procuraduría de Protección a Niñas, Niños y Adolescentes

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Niveles de Seguridad de los Datos Personales	Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, 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 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.

Procuraduría de Protección a Niñas, Niños y Adolescentes

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD

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 Procuraduría 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
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titolares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policía 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 Procuraduría 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: • Luis Antonio Gómez Hurtado, Procurador 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; • Víctor Hugo Escalante Juárez, Director de Representación y Restitución; • María Raquel Arias Covarrubias; Directora de Tutela de Derechos; • Eunice Adriana Avilés Valencia, Directora del CEPAVI;
Procedimientos de respaldo y recuperación de datos personales	Ademas del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.

Procuraduría de Protección a Niñas, Niños y Adolescentes

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	Tipo de capacitación	Tipo de personal
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 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, los datos de procedimientos jurídicos, bienes muebles o inmuebles, fiscales, ingresos.
Niveles de Seguridad de los **Datos Personales**		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Dirección Jurídica

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • Datos ideológicos: Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • Datos de salud: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • Características biométricas: Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • Vida sexual: Preferencia sexual, hábitos sexuales, entre otros. • Origen: Étnico y racial.
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 bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha

Dirección Jurídica

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
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
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 Departamento 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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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.

Dirección Jurídica

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
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		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Órgano Interno de Control

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Órgano Interno de Control
Respecto del administrador de éste	Nombre	Juana Elizabeth Guzmán Elías
	Cargo	Titular del Órgano Interno de Control
	Adscripción	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 Proteccion 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 juridicos 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 Proteccion de Datos Personales del Sistema DIF Jalisco, asi lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**Datos Personales.** Nombre, edad, sexo, firma, Caracteristicas fisicas, morales, domicilio particular, número de telefono particular, Clave Única de Registro de Población, Registro Federal de Contribuyentes, los datos de procedimientos juridicos, bienes muebles o inmuebles, fiscales, ingresos.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de Justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Órgano Interno de Control

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias toxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada físicamente en expedientes cerrados, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Órgano Interno de Control.
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 bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros del Órgano Interno de Control, 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 alfanumericas de alta seguridad

Órgano Interno de Control

FICHA DE PRDTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
Gestión de vulneraciones
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 las oficinas del Órgano Interno de Control son: • Juana Elizabeth Guzmán Elías, Titular del Órgano Interno de Control;
Procedimientos de respaldo y recuperación de datos personales	Se cuenta en expediente físico.
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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 este 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		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**

Órgano Interno de Control

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 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 de la Dirección de Recursos Humanos
Respecto del administrador de éste	Nombre	Aurora Carolina González Hidalgo
	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 laborales, bienes muebles e inmuebles. **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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Dirección de Recursos Humanos

FICHA DE PROTECCIÓN DE DATDS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros del 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 alfanumericas de alta seguridad.

Dirección de Recursos Humanos

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
Gestión de vulneraciones
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 actiuidades, 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: • Aurora Carolina González Hidalgo, Directora de Recursos Humanos; • Yuriria Jazmín Tonanzing Rios Gutiérrez, Administración de Personal; • Yesika Nayeli Gutiérrez Jiménez, Prestaciones y Servicio Social;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**

Dirección de Recursos Humanos

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Dirección de Recursos Financieros

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTD 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.
Niveles de Seguridad de los Datos **Personales**		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Dirección de Recursos Financieros

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • Datos ideológicos: Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • Datos de salud: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • Características biométricas: Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • Vida sexual: Preferencia sexual, hábitos sexuales, entre otros. • Origen: Étnico y racial.
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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas).

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

Dirección de Recursos Financieros

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
Gestión de vulneraciones
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 Dominguez, Presupuestos; • Luz Angélica López Ortiz, Contabilidad; • Gildardo Mendoza Juárez. Tesoreria;
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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	Tipo de capacitación	Tipo de personal

Dirección de Recursos Financieros

FICHA DE PRDTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 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	Roberto Alejandro Valladares Zamudio
	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
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Dirección de Recursos Materiales

FICHA OE PROTECCIÓN DE OATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial
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
Cunsiderando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismu, 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 u 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 policía custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.

Dirección de Recursos Materiales

FICHA DE PRDTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
Gestión de vulneraciones
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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: • Roberto Alejandro Valladares Zamudio, Director de Recursos Materiales; • Alberto Clemente Preciado García, Activos Fijos; • Esther Fausto Brito, Almacén;
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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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 administ ador 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		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**

Dirección de Recursos Materiales

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Dirección de Planeación Institucional

FICHA DE PRDTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Planeación Institucional
Respecto del administrador de éste	**Nombre**	Ernesto Jesús Ivon Pliego
	Cargo	Director de Planeación Institucional
	Adscripción	Dirección de Planeación Institucional
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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales**: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros

Dirección de Planeación Institucional

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen**: Étnico y racial.
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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en 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

Dirección de Planeación Institucional

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 Institucional son: • Ernesto Jesús Ivon Pliego, Director de Planeación Institucional; • Héctor Juárez Ayard; Jefe de Departamento de Planeación y Desarrollo de Proyectos;
Procedimientos de respaldo y recuperación de datos personales	Los archivos se encuentra en formatos digitales en cuentas asociadas al correo institucional.
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	Tipo de capacitación	Tipo de personal

Dirección de Planeación Institucional

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 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 de la Dirección de Servicios Generales
Respecto del administrador de éste	**Nombre**	Jose Manuel Castellanos Bustos
	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, datos laborales. Datos Personales Sensibles.- datos biométricos.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Dirección de Servicios Generales

FICHA DE PRDTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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 area, 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.

Dirección de Servicios Generales

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
Gestión de vulneraciones
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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: • Jose Manuel Castellanos Bustos, Director de Servicios Generales; • Iván González Neri, Jefe del Departamento de Servicios Diversos; • Jorge Alejandro Beleche Morales, Jefe del Departamento de Mantenimiento; • Salvador Morales Yera, Jefe del Departamento de Transportes;
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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	Tipo de capacitación	Tipo de personal

Dirección de Servicios Generales

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 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 Informaticos
Respecto del administrador de éste	Nombre	Hernán Velasco Vélez
	Cargo	Director de Tecnologías y Sistemas Informaticos
	Adscripción	Dirección de Tecnologías y Sistemas Informaticos
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 generales de su domicilio con cruces y colonia, así como municipio de nacimiento, integrantes de la familia, ingreso familiar mensual, datos laborales.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales**: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Dirección de Tecnologías y Sistemas de Información

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran 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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los 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 policía custodiando instalaciones.
Gestión de vulneraciones

Dirección de Tecnologías y Sistemas de Información

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Tecnologías y Sistemas de Información son: • Hernán Velasco Vélez, Director de Tecnologías y Sistemas de Información; • Jorge Chavez Ruiz, Jefe del Departamento de Infraestructura Tecnológica; • Jonathan Alfonso Jiménez Vázquez, Jefe del Departamento de Calidad en Información; • Irasema Lilian Osuna Chávez, Jefe del Departamento de Soporte Técnicu;
Procedimientos de respaldo y recuperación de datos personales	Se tiene resguardada la información en el Servidor del Organismo.
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o perdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Dirección de Tecnologías y Sistemas de Información

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Fecha de actualización del documento de seguridad	Noviembre del 2019

Dirección de Trabajo Social

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Trabajo Social
Respecto del administrador de éste	Nombre	María Eugenia Gutiérrez Solís
	Cargo	Directora de Trabajo Social
	Adscripción	Dirección de Trabajo Social
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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Dirección de Trabajo Social

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, 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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas). 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 neresario trasladarlos a un area comun, para mejor control y seguimiento

Análisis de brecha

Dirección de Trabajo Social

FICHA DE PRDTECCIÓN DE DATOS PERSDNALES

DOCUMENTO DE SEGURIDAD
Los expedientes se encuentran en archiveros de la Direcciún, 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
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 son: • María Eugenia Gutiérrez Solís, Directora de Trabajo Social; • 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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encventra sujeto a modificaciones de conformidad con el plan de trabajo.
Técnicas utilizadas para la supresión y borrado segura 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		
Temporalidad	Tipo de capacitación	Tipo de personal

Dirección de Trabajo Social

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Dirección de Atención a las Personas Adultas Mayores

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 las Personas Adultas Mayores
Respecto del administrador de éste	**Nombre**	María Asensión Álvarez Solís
	Cargo	Directora de Atención a las Personas Adultas Mayores
	Adscripción	Dirección de Atención a las Personas Adultas Mayores
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.
Niveles de Seguridad de los **Datos Personales**		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Dirección de Atención a las Personas Adultas Mayores

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha

Dirección de Atención a las Personas Adultas Mayores

FICHA DE PRDTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIOAD
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
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa uean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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, Jefe del Departamento de Estrategias de Atención a las Personas Adultas Mayores; • Angelica Contreras Robles, Jefa del Departamento de Gestión de Centros de Atención a Personas Adultas Mayores;
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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirian restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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

Dirección de Atención a las Personas Adultas Mayores

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
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		
Temporalidad	**Tipo de capacitación**	Tipo de personal
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesion de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Dirección de Atención a la Infancia

FICHA DE PRDTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Atención a la Infancia
Respecto del administrador de éste	Nombre	José Martín Díaz de León Díaz de León
	Cargo	Director de Atención a la Infancia
	Adscripción	Dirección de Atención a la 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, Nacionalidad. **Datos Personales Sensibles.** Estado de salud física y mental, historial médico, información genética, creencias religiosas, filosóficas u morales.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.
		Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros • **Origen:** Étnico y racial.
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		

Dirección de Atención a la Infancia

FICHA DE PRDTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
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
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 metálicas 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 metálicas 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 Infancia son: • José Martín Díaz de León Díaz de León, Director de Atención a la Infancia; • Tania Yahaira Ramírez De La Rocha, Jefa del Departamento de Gestión en Centros de Atención Infantil;
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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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 realizaran 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		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Dirección de Atención a 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 de Atención a Personas con Discapacidad
Respecto del administrador de éste	Nombre	Jehu Jonathan Preciado Pérez
	Cargo	Director de Atención a Personas con Discapacidad
	Adscripción	Dirección de Atención a 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 mandatu 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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales**: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratadus, referencias personales, entre otros • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Dirección de Atención a Personas con Discapacidad

FICHA DE PROTECCION DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. ▪ **Características biométricas:** Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. ▪ **Origen:** Étnico y racial.
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, 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.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva, El daño, la alteración o modificación no autorizada y Observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de 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 computo y de respaldn seguro de informacion, (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 policía custodiando instalaciones, algunos equipos de compuzo carecen de contraseñas alfanumericas de alta seguridad.

Dirección de Atención a Personas con Discapacidad

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
Gestión de vulneraciones
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimuniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 de Atención a Personas con Discapacidad son: • Jehu Jonathan Preciado Pérez, Dirección de Atención a Personas con Discapacidad; • Liliana Arcelia Gutierrez Gómez, Jefa del Departamento de Estrategias de Atención a Personas con Discapacidad;
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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, asi como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirian restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**

Dirección de Atención a Personas con Discapacidad

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados, • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Dirección de Atención a Personas en Situación de Emergencia

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 Personas en Situación de Emergencia
Respecto del administrador de éste	**Nombre**	Luis Rosendo Rodriguez Peña
	Cargo	Director de Atención a Personas en Situación de Emergencia
	Adscripción	Dirección de Atención a Personas en Situación de Emergencia
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 confidenclalidad** 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, teléfono particular, teléfono celular, estado civil, firma, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales, datos de tránsito y movimientos migratorios. **Datos Personales Sensibles.-** Estado de salud, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, tipo de sangre, ADN, huella dactilar u otros análogos, olor de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, origen étnico y racial.
		Nivel de Seguridad Básica: • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

Dirección de Atención a Personas en Situación de Emergencia

FICHA DE PROTECCIÓN DE DATDS PERSONALES

DOCUMENTO DE SEGURIDAD	
Niveles de Seguridad de los Datos Personales	Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, 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.

Dirección de Atención a Personas en Situación de Emergencia

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
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 o 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
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 Atención a Personas en Situación de Emergencia son: • Luis Rosendo Rodriguez Peña, Director de Atención a Personas en Situación de Emergencia; • Jose Guadalupe Prado Ortega Jefe del Departamento de Desarrollo Integral para Personas en Situación de Calle; • Taoki Catalina Gonzalez Mariscal, Jefa del Departamento de Red de Comunidades Solidarias
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.

Dirección de Atención a Personas en Situación de Emergencia

FICHA DE PRDTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	Tipo de capacitación	Tipo de personal
Semestral	▪ Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; ▪ Principios y deberes que deben observarse en el tratamiento de los datos personales; y ▪ Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Dirección de Comedores y Centros de Distribución de Alimentos

FICHA DE PROTECCIÓN DE DATOS PERSDNALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Comedores y Centros de Distribución de Alimentos
Respecto del administrador de éste	**Nombre**	Herlinda Álvarez Arreola
	Cargo	Directora de Comedores y Centros de Distribución de Alimentos
	Adscripción	Dirección de Comedores y Centros de Distribución de Alimentos
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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Dirección de Comedores y Centros de Distribución de Alimentos

FICHA DE PRDTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, así como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en 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 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 expedience 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 alfanumericas de alta seguridad.
Gestión de vulneraciones

Dirección de Comedores y Centros de Distribución de Alimentos

FICHA DE PRDTECCIÓN DE DATDS PERSONALES

DOCUMENTO DE SEGURIDAD
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboracion de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 Comedores y Centros de Distribución de Alimentos son: •Herlinda Álvarez Arreola, Directora de Comedores y Centros de Distribución de Alimentos; • Alejandra Maytorena Sandoval, Jefa del Departamento de Nutrición Escolar; • Karen Joanna Lizbeth Patiño Hurtado, Jefa del Departamento de 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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	Tipo de capacitación	Tipo de personal

Dirección de Comedores y Centros de Distribución de Alimentos

FICHA DE PROTECCIÓN DE DATDS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Dirección de Vinculación 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 Vinculación Municipal
Respecto del administrador de éste	Nombre	Teresa Luna Palafox
	Cargo	Directora de Vinculación Municipal
	Adscripción	Dirección de Vinculación 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, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, idioma.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros • **Datos laborales**: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros. **Nivel de Seguridad Media:** • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros

Dirección de Vinculación Municipal

FICHA DE PROTECCIÓN DE DATDS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, 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.
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

Dirección de Vinculación Municipal

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
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 alfanumericas de alta seguridad.

Gestión de vulneraciones
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 Vinculación Municipal son: • Israel González Ramírez, Subdirector General de Desarrollo Comunitario y Apoyo Municipal • Teresa Luna Palafox, Dirección de Vinculación Municipal; • Yadira Larios Preciado, Jefa del Departamento de Zona Norte; • Anna Elizabeth Ramírez Mares, Jefa del Departamento de Zona Centro; • Alba Rosa Azpeitia Sanchez, Jefa del Departamento de 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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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 Proteccion de Datos Personales del Sistema DIF Jalisco.

Dirección de Vinculación Municipal

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIOAD	
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		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Dirección de Control de la Gestión Institucional

FICHA DE PRDTECCIÓN DE DATDS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Control de la Gestión Institucional
Respecto del administrador de éste	Nombre	Jorge Armando González Muñoz
	Cargo	Director de Control de la Gestión Institucional
	Adscripción	Dirección de Control de la Gestión Institucional
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 Persanales.- Nombre, domicilio particular, número de teléfono particular, correo electrónico particular, Clave Única de Registro de Población, Registro Federal de Contribuyentes, fotografía, laborales.
Niveles de Seguridad de los Datos Personales		Nivel de Seguridad Básica: • Datos de identificación: Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • Datos laborales: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • Datos patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdicdonales: información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • Datos académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Dirección de Control de la Gestión Institucional

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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

Dirección de Control de la Gestión Institucional

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
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 alfanumericas de alta seguridad.

Gestión de vulneraciones
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 Control de la Gestión Institucional son: •Jorge Armando González Muñoz, Director de Control de la Gestión Institucional • Pedro Pablo López Martínez, Jefe del Departamento de Relaciones Públicas; • Adriana Zabalgoitia Ibarra, Jefa del Departamento Comunicación Social;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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 cunsiderarlo 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

Dirección de Control de la Gestión Institucional

FICHA DE PROTECCIÓN DE DATDS PERSONALES

DOCUMENTO DE SEGURIDAD		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 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	Silvia Briseño Muñoz
	Cargo	Jefa de departamento del C.A.D.I 2
	Adscripción	Centro Asistencial de Desarrollo Infantil numero 02
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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidas en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, 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 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 sería: la pérdida o destrucción, robo, extravío u 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

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
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
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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. D2 son: • Silvia Briseño Muñoz, Jefa del Departamento de C.A.D.I. D2;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos basicos 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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del ultimo respaldo El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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	Verificacion 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

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Temporalidad	**Tipo de capacitación**	Tipo de personal
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 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 No. 6
Respecto del administrador de éste	Nombre	Luz Elena Pérez Guzmán
	Cargo	Director de Atención a la Infancia
	Adscripción	Dirección de Atención a la 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, 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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros. **Nivel de Seguridad Media:** • Datos patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta coma parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Centros de Atención de Desarrollo Infantil

FICHA DE PRDTECCIÓN DE DATDS PERSDNALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, 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 resguarda 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 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 Organisma, 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

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
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
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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. 06 son: • Luz Elena Pérez Guzmán, Jefa de departamento del C.A.D.I. 6
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	Tipo de capacitación	Tipo de personal

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 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	Jefa 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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite. • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipn de sangre, ADN, huella dactilar color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, así como a aquellas autoridades federales y/o estatales y/o municipales, que cunforme 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 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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia. (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computn 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.

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
Gestión de vulneraciones
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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. 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 datos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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		
Temporalidad	Tipo de capacitación	Tipo de personal

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 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	Jefa 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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite. • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, 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 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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros de 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.

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
Gestión de vulneraciones
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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	Verificacion 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		
Temporalidad	Tipo de capacitación	Tipo de personal

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 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	Jefa 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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales**: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite. • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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, 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 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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas).

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

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATDS PERSONALES

DOCUMENTO DE SEGURIDAD
Gestión de vulneraciones
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en dunde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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 verificara 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		
Temporalidad	Tipo de capacitación	Tipo de personal

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Fecha de actualización del documento de seguridad	Noviembre del 2019

Casa Hogar para Personas en Situación de Calle

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Casa Hogar para Personas en Situación de Calle
Respecto del administrador de éste	Nombre	Aldo Tonatiuh Nino Laungren
	Cargo	Coordinardor Administrativo
	Adscripción	Casa Hogar para Personas en Situación de Calle
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, teléfono particular, teléfono celular, estado civil, firma, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales, datos de tránsito y movimientos migratorios. **Datos Personales Sensibles.-** Estado de salud, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, tipo de sangre, ADN, huella dactilar u otros análogos, olor de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, origen étnico y racial.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros

Casa Hogar para Personas en Situación de Calle

FICHA DE PROTECCIÓN DE DATOS PERSDNALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar, color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen**: Étnico y racial.
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, 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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizadu, 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 Casa Hogar, 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.

Casa Hogar para Personas en Situación de Calle

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
Gestión de vulneraciones
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 Atención a Personas en Situación de Emergencia son: • Aldo Tonatiuh Nino Laungren, Coordinador Administrativo.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
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 administ ador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán pro uestas 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		
Temporalidad	Tipo de capacitación	Tipo de personal
ercer trim	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Casa Hogar para Personas en Situación de Calle

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Fecha de actualización del documento de seguridad	Noviembre del 2019

Archivo de Concentración 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	Luis Alan Rodríguez Ortega
	Cargo	Coordinador Administrativo "A"
	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.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales:** Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Archivo de Concentración del Sistema DIF Jalisco y sus Órganos Desconcentrados

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
	Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen:** Étnico y racial.
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 sería: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que 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 los estantes del archivo, 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

Archivo de Concentración del Sistema DIF Jalisco y sus Órganos Desconcentrados

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD
• Restauración inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

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 son tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingresa 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 el Archivo de Concentración son: • Luis Alan Rodríguez Ortega, Coordinador Administrativo A; • Ana Margarita Vázquez Medina, Analista Especializado; • José de Jesús Segura de León, Jefe de Departamento de la Unidad de Transparencia;
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 misma contiene.
Plan de contingencia	En caso de cualquier vulneración a daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo
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 este 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 encargada de Pratección de Datos Personales de DIF Jalisco, que se cumpla con las medidas de seguridad consignadas en el presente documento

Programa General de capacitación		
Temporalidad	Tipo de capacitación	Tipo de personal
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos

Archivo de Concentración del Sistema DIF Jalisco y sus Órganos Desconcentrados

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Fecha de actualización del documento de seguridad	Noviembre del 2019

BITACORA DE ACCESO Y OPERACION 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 de 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

AVISO DE PRIVACIDAD CORTO

El **Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco (Sistema DIF Jalisco),** con domicilio en Av. Alcalde número 1220, colonia Miraflores en Guadalajara, Jalisco, hace de su conocimiento que se consideraran como datos personales la información concerniente a una persona física identificada o identificable, y por datos personales sensibles, aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste; datos que podrán ser sometidos a tratamiento única y exclusivamente para los fines que fueron proporcionados, de acuerdo a las finalidades y atribuciones establecidas en el numeral 16 párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, así como lo dispuesto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Los titulares de los datos personales tienen el derecho de conocer sobre el tratamiento que se les dará a los datos proporcionados al **Sistema DIF Jalisco**, mediante los Avisos de Privacidad que se encuentran en cada uno de los accesos de los inmuebles de la Institución y a través de medios electrónicos por los que se recaban datos personales, a fin de tomar decisiones informadas al respecto.

El aviso de privacidad en sus modalidades: integral, simplificado y corto, están disponibles para su libre acceso y consulta en la página de internet de este sujeto obligado, la cual es: http://sistemadif.jalisco.gob.mx/sitio2013/, del mismo modo en nuestro Portal de Transparencia en su Artículo 8, Fracciones VIII y IX, https://transparencia.info.jalisco.gob.mx/transparencia/informacion-fundamental/12337.

Fecha de Actualización: *Noviembre de 2019.*

AVISO DE SIMPLIFICADO

El **Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco (Sistema DIF Jalisco),** con domicilio en Av. Alcalde número 1220, colonia Miraflores en Guadalajara, Jalisco, es el responsable del uso y protección de sus datos personales, y al respecto le informa lo siguiente:

Los datos personales, se refieren a la información concerniente a una persona física identificada o identificable, y por datos personales sensibles, aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste.

Los datos personales que usted proporcione al **Sistema DIF Jalisco** serán única y exclusivamente utilizados para llevar a cabo los objetivos y atribuciones de este Organismo asistencial, y los utilizaremos para la integración de expedientes derivados de la atención o servicios que requiera usted como usuario de éste, dándole el tratamiento de protección, los cuales serán almacenados con las medidas de seguridad necesarias.

Con relación a la transferencia de su información, los terceros receptores de los datos personales pueden ser *Autoridades Judiciales, el Agente del Ministerio Público, la Auditoría Superior del Estado con la finalidad de dar atención a los requerimientos judiciales o legales, a los Sistemas DIF Municipales del Estado de Jalisco con la finalidad de dar seguimiento a programas o servicios, el Instituto de Transparencia Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI) para cumplir con las obligaciones de transparencia, las autoridades Federales, Estatales y Municipales, siempre que los datos se utilicen para el ejercicio de sus facultades y atribuciones.*

Los datos personales recabados, podrán ser tratados sin consentimiento del titular, siempre en respeto a sus derechos; teniendo como supuestos de excepción a los principios que rigen el tratamiento de datos según lo establece el segundo párrafo del artículo 16, de la Constitución Política de los Estados Unidos Mexicanos, así como en los supuestos consagrados en artículo 75 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Jalisco.

Usted en cualquier momento puede solicitar su *Acceso, Rectificación, Cancelación,*

Tel. 3030 3800
01 800 3000 342
Av. Alcalde # 1220
Colonia Miraflores, C.P. 44270
Guadalajara, Jalisco, México

Oposición o Revocación del consentimiento, mediante la presentación de una solicitud de ejercicio de *derechos ARCO*, ante la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, ubicada en Avenida Alcalde número 1220, Colonia Miraflores, Guadalajara Jalisco, por correo electrónico oficial transparencia@difjalisco.gob.mx, *teniendo un horario de 09:00 a 15:00 horas*, de igual manera está a su disposición, vía internet, la Plataforma Nacional de Transparencia (PNT).

El aviso de privacidad en sus modalidades: integral, simplificado y corto, están disponibles para su libre acceso y consulta en la página de internet de este sujeto obligado, la cual es: http://sistemadif.jalisco.gob.mx/sitio2013/, del mismo modo en nuestro Portal de Transparencia en su 8 Fracciones VIII y IX, https://transparencia.info.jalisco.gob.mx/transparencia/informacion-fundamental/12337.

Fecha de Actualización: *Noviembre de 2019.*

AVISO DE PRIVACIDAD INTEGRAL

El **Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco (Sistema DIF Jalisco),** con domicilio en Av. Alcalde número 1220, colonia Miraflores en Guadalajara, Jalisco, es el responsable del uso y protección de sus datos personales, y al respecto le informa lo siguiente:

Los datos personales, aquellos que se refieren a la información concerniente a una persona física identificada o que la hace identificable, así mismo son parte esencial de la identidad de un individuo, puesto que éstos permiten hacer una referencia exacta y objetiva para particularizar a una persona y hacerla sujeta de derechos y obligaciones, y por datos personales sensibles, aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste.

El tratamiento de sus datos personales se realiza con fundamento en los artículos 1, 6 apartado A, fracciones II y III, así como el 16 párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 4, 7 en su párrafo segundo, 9 fracción V, de la Constitución Política del Estado de Jalisco; artículo 3 fracciones II y III, 20, 21, 22, 23, 24, 25, 26, 27 y 28 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; el 15, 19, 20, 21, 22, 24 punto 1, 25, 26, 75, 85 y 86 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Jalisco; el 25 del Código de Asistencia Social del Estado de Jalisco; los artículos 20, 21, 22, 23 fracciones II y III, 24 fracciones V y 25 fracciones XV, XVII y XX, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; el artículo 17 fracciones I, III, IV, V, VII y XII, 44, 54 BIS-4, 54 BIS-5 y 56 de la Ley para los Servidores Públicos del Estado de Jalisco y sus Municipios; el 2 fracciones III y 53 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

Los datos personales que serán sometidos a tratamiento son: *nombre, domicilio y número de teléfono particular, edad, fecha y lugar de nacimiento, nacionalidad, identificación oficial, Clave Única de Registro de Población, Registro Federal de Contribuyentes, ultimo grado de estudios, estado civil, firma autógrafa, correo electrónico personal, así mismo se utilizarán datos personales considerados como sensibles, que*

requieren de un manejo especial como son: vida afectiva o familiar, origen étnico o racial, características físicas, morales o emocionales imagen, fotografía, video, patrimonio, ideología, opinión política, afiliación sindical, creencia o convicción religiosa y filosófica, datos biométricos, estado de salud física y mental, historial médico, preferencia sexual, otras análogas que afecten su intimidad, que pueda dar origen a discriminación o que su difusión o entrega a terceros conlleve a un riesgo para su titular y además la considerada como confidencial por disposición legal.

Los datos personales que usted proporcione al **Sistema DIF Jalisco**, serán única y exclusivamente utilizados para llevar a cabo los objetivos y atribuciones de este Organismo asistencial y los utilizaremos para su *identificación, localización, acreditar el cumplimiento de los criterios de elegibilidad establecidos en las reglas de operación de los diferentes programas a cargo del sistema, llevar a cabo procesos jurídicos, la contratación de servicios personales, integrar expedientes del personal, comprobar el uso adecuado de los recursos de los programas asignados, estatales y federales, tener un registro de las personas atendidas, para salvaguardar la integridad y seguridad de las y los trabajadores, así como de las y los ciudadanos que ingresan a las instalaciones del organismo asistencial*, los cuales pueden ser recabados de manera directa o indirecta, medios electrónicos, escrito y vía telefónica; La información que nos proporcione, estará bajo resguardo y protegida por este, dándole el tratamiento de protección de datos sensibles, los cuales serán almacenados con las medidas de seguridad necesarias.

Con relación a la transferencia de su información los terceros receptores de los datos personales pueden ser *Autoridades Judiciales, el Agente del Ministerio Público, la Auditoría Superior del Estado con la finalidad de dar atención a los requerimientos judiciales o legales, a los Sistemas DIF Municipales del Estado de Jalisco con la finalidad de dar seguimiento a programas o servicios, el Instituto de Transparencia Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI) para cumplir con las obligaciones de transparencia, las autoridades Federales, Estatales y Municipales, siempre que los datos se utilicen para el ejercicio de sus facultades y atribuciones*.

Los datos personales recabados, podrán ser tratados sin consentimiento del titular, siempre en respeto a sus derechos; teniendo como supuestos de excepción a los principios que rigen el tratamiento de datos, la seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros,

según lo establece el segundo párrafo del artículo 16, de la Constitución Política de los Estados Unidos Mexicanos, así como en los supuestos consagrados en artículo 15 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Jalisco, en los casos que se requieran del consentimiento del titular que no se realizarán transferencias de datos personales.

Usted en cualquier momento puede solicitar su *Acceso, Rectificación, Cancelación, Oposición o Revocación del consentimiento*, mediante la presentación de una solicitud de ejercicio de *derechos ARCO*, ante la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, ubicada en Avenida Alcalde número 1220, Colonia Miraflores, Guadalajara Jalisco, por correo electrónico oficial transparencia@difjalisco.gob.mx, *teniendo un horario de 09:00 a 15:00 horas*, de igual manera está a su disposición, vía internet, la Plataforma Nacional de Transparencia (PNT).

Cualquier cambio al presente aviso de privacidad se hará del conocimiento de los titulares de la información confidencial, a través de la página de internet de este sujeto obligado, la cual es: http://sistemadif.jalisco.gob.mx/sitio2013/, del mismo modo en nuestro Portal de Transparencia en su Artículo 8 Fracciones VIII y IX, https://transparencia.info.jalisco.gob.mx/transparencia/informacion-fundamental/12337.

Fecha de Actualización: *Noviembre de 2019.*

Tel 3030 3900
01 800 3000 344
Av. Alcalde # 1220
Colonia Miraflores CP 44270
Guadalajara, Jalisco, México

AVISO DE PRIVACIDAD CORTO

El **Consejo Estatal para la Prevención y Atención de la Violencia Familiar (CEPAVI)**, órgano desconcentrado del **Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco (Sistema DIF Jalisco)**, con domicilio en Av. Américas número 599, Torre Cuauhtémoc, Col. Ladrón de Guevara, C.P. 44600, Guadalajara, Jalisco, hace de su conocimiento que se consideraran como datos personales la información concerniente a una persona física identificada o identificable, y por datos personales sensibles, aquellos que afecten a la esfera más intima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste; datos que podrán ser sometidos a tratamiento única y exclusivamente para los fines que fueron proporcionados, de acuerdo a las finalidades y atribuciones establecidas en el numeral 16 párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, así como lo dispuesto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Los titulares de los datos personales tienen el derecho de conocer sobre el tratamiento que se les dará a los datos proporcionados al **Consejo**, mediante los Avisos de Privacidad que se encuentran en cada uno de los accesos de los inmuebles de la Institución y a través de medios electrónicos por los que se recaban datos personales, a fin de tomar decisiones informadas al respecto.

El aviso de privacidad en sus modalidades: integral, simplificado y corto, están disponibles para su libre acceso y consulta en nuestro Portal de Transparencia en su Artículo 8, Fracciones VIII y IX, https://transparencia.info.jalisco.gob.mx/transparencia/informacion-fundamental/12337.

Fecha de Actualización: *Noviembre de 2019*

AVISO DE SIMPLIFICADO

El **Consejo Estatal para la Prevención y Atención de la Violencia Familiar (CEPAVI)**, órgano desconcentrado del **Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco (Sistema DIF Jalisco)**, con domicilio en Av. Américas número 599, Torre Cuauhtémoc, Col. Ladrón de Guevara, C.P. 44600, Guadalajara, Jalisco, es el responsable del uso y protección de sus datos personales, y al respecto le informa lo siguiente:

Los datos personales, se refieren a la información concerniente a una persona física identificada o identificable, y por datos personales sensibles, aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste.

Los datos personales que usted proporcione al **Consejo Estatal para la Prevención y Atención de la Violencia Familiar (CEPAVI)** serán única y exclusivamente utilizados para llevar a cabo los objetivos y atribuciones de este Organismo y los utilizaremos para la integración de expedientes derivados de la atención o servicios que requiera usted como usuario de éste, dándole el tratamiento de protección, los cuales serán almacenados con las medidas de seguridad necesarias.

Con relación a la transferencia de su información, los terceros receptores de los datos personales pueden ser *Autoridades Judiciales, el Agente del Ministerio Público, la Auditoría Superior del Estado con la finalidad de dar atención a los requerimientos judiciales o legales, a los Sistemas DIF Municipales del Estado de Jalisco con la finalidad de dar seguimiento a programas o servicios, el Instituto de Transparencia Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI) para cumplir con las obligaciones de transparencia, las autoridades Federales, Estatales y Municipales, siempre que los datos se utilicen para el ejercicio de sus facultades y atribuciones.*

Los datos personales recabados, podrán ser tratados sin consentimiento del titular, siempre en respeto a sus derechos; teniendo como supuestos de excepción a los principios que rigen el tratamiento de datos según lo establece el segundo párrafo del artículo 16, de la Constitución Política de los Estados Unidos Mexicanos, así como en los supuestos consagrados en artículo 75 de la Ley de Protección de Datos Personales

en Posesión de los Sujetos Obligados para el Estado de Jalisco.

Usted en cualquier momento puede solicitar su *Acceso, Rectificación, Cancelación, Oposición o Revocación del consentimiento*, mediante la presentación de una solicitud de ejercicio de *derechos ARCO*, ante la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, ubicada en Avenida Alcalde 1220, Colonia Miraflores, Guadalajara Jalisco por correo electrónico oficial transparencia@difjalisco.gob.mx, *teniendo un horario de 09:00 a 15:00 horas*, de igual manera está a su disposición vía internet, la Plataforma Nacional de Transparencia (PNT).

El aviso de privacidad en sus modalidades: integral, simplificado y corto están disponibles para su libre acceso y consulta en nuestro Portal de Transparencia en su Artículo 8, Fracciones VIII y IX, https://transparencia.info.jalisco.gob.mx/transparencia/informacion-fundamental/12337.

Fecha de Actualización: *Noviembre de 2019.*

AVISO DE PRIVACIDAD INTEGRAL

El **Consejo Estatal para la Prevención y Atención de la Violencia Familiar (CEPAVI)**, órgano desconcentrado del **Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco (Sistema DIF Jalisco)**, con domicilio en Av. Américas número 599, Torre Cuauhtémoc, Col. Ladrón de Guevara, C.P. 44600, Guadalajara, Jalisco, es el responsable del uso y protección de sus datos personales, y al respecto le informa lo siguiente:

Los datos personales, aquellos que se refieren a la información concerniente a una persona física identificada o que la hace identificable, así mismo son parte esencial de la identidad de un individuo, puesto que éstos permiten hacer una referencia exacta y objetiva para particularizar a una persona y hacerla sujeta de derechos y obligaciones; y por datos personales sensibles, aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste.

El tratamiento de sus datos personales se realiza con fundamento en los artículos 1, 6 apartado A, fracciones II y III, así como el 16 párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 4, 7 en su párrafo segundo, 9 fracción V, de la Constitución Política del Estado de Jalisco; artículo 3 fracciones II y III, 20, 21, 22, 23, 24, 25, 26, 27 y 28 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; el 15, 19, 20, 21, 22, 24 punto 1, 25, 26, 75, 85 y 86 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Jalisco; los 25 y 41 del Código de Asistencia Social del Estado de Jalisco; los artículos 20, 21, 22, 23 fracciones II y III, 24 fracciones V y 25 fracciones XV, XVII y XX, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; el artículo 17 fracciones I, III, IV, V, VII y XII, 44, 54 BIS-4, 54 BIS-5 y 56 de la Ley para los Servidores Públicos del Estado de Jalisco y sus Municipios; el 2 fracciones III; 14 y 20 de la Ley para la Prevención y Atención de la Violencia Intrafamiliar del Estado de Jalisco y 53 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

Los datos personales que serán sometidos a tratamiento son *nombre, domicilio y número de teléfono particular, edad, fecha y lugar de nacimiento, nacionalidad, identificación oficial, Clave Única de Registro de Población, Registro Federal de*

Contribuyentes, ultimo grado de estudios, estado civil, firma autógrafa, correo electrónico personal, así mismo se utilizarán datos personales considerados como sensibles, que requieren de un manejo especial como son: vida afectiva o familiar, origen étnico o racial, características físicas, morales o emocionales, imagen, fotografía, video, patrimonio, ideología, opinión política, afiliación sindical, creencia o convicción religiosa y filosófica, datos biométricos, estado de salud física y mental, historial médico, preferencia sexual, otras análogas que afecten su intimidad, que pueda dar origen a discriminación o que su difusión o entrega a terceros conlleve a un riesgo para su titular y además la considerada como confidencial por disposición legal.

Los datos personales que usted proporcione al **CEPAVI,** serán única y exclusivamente utilizados para llevar a cabo los objetivos y atribuciones de este Organismo y los utilizaremos para para su *identificación, localización, acreditar el cumplimiento de los criterios de elegibilidad establecidos en las reglas de operación de los diferentes programas a cargo del sistema, llevar a cabo procesos jurídicos, la contratación de servicios personales, integrar expedientes del personal, comprobar el uso adecuado de los recursos de los programas asignados, estatales y federales, tener un registro de las personas atendidas, para salvaguardar la integridad y seguridad de las y los trabajadores, así como de las y los ciudadanos que ingresan a las instalaciones del organismo asistencial*, los cuales pueden ser recabados de manera directa o indirecta, medios electrónicos, escrito y vía telefónica; La información que nos proporcione, estará bajo resguardo y protegida por este, dándole el tratamiento de protección de datos sensibles, los cuales serán almacenados con las medidas de seguridad necesarias.

Con relación a la transferencia de su información los terceros receptores de los datos personales pueden ser *Autoridades Judiciales, el Agente del Ministerio Público, la Auditoría Superior del Estado con la finalidad de dar atención a los requerimientos judiciales o legales, a los Sistemas DIF Municipales del Estado de Jalisco con la finalidad de dar seguimiento a programas o servicios, el Instituto de Transparencia Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI) para cumplir con las obligaciones de transparencia, las autoridades Federales, Estatales y Municipales, siempre que los datos se utilicen para el ejercicio de sus facultades y atribuciones.*

Los datos personales recabados, podrán ser tratados sin consentimiento del titular, siempre en respeto a sus derechos; teniendo como supuestos de excepción a los principios que rigen el tratamiento de datos, la seguridad nacional, disposiciones de

orden público, seguridad y salud públicas o para proteger los derechos de terceros, según lo establece el segundo párrafo del artículo 16, de la Constitución Política de los Estados Unidos Mexicanos, así como en los supuestos consagrados en artículo 15 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Jalisco, en los casos que se requieran del consentimiento del titular que no se realizarán transferencias de datos personales.

Usted en cualquier momento puede solicitar su *Acceso, Rectificación, Cancelación, Oposición o Revocación del consentimiento*, mediante la presentación de una solicitud de ejercicio de *derechos ARCO*, ante la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, ubicada en Avenida Alcalde número 1220, Colonia Miraflores, Guadalajara Jalisco, por correo electrónico oficial transparencia@difjalisco.gob.mx, *teniendo un horario de 09:00 a 15:00 horas*, de igual manera está a su disposición, vía internet, la Plataforma Nacional de Transparencia (PNT).

Cualquier cambio al presente aviso de privacidad se hará del conocimiento de los titulares de la información confidencial, a través del Portal de Transparencia en su Artículo 8 Fracciones VIII y IX, https://transparencia.info.jalisco.gob.mx/transparencia/informacion-fundamental/12337.

Fecha de Actualización: *Noviembre de 2019.*

Tel. (33) 3030 3800
01 800 3000 343
Av. Alcalde # 1229
Colonia Miraflores, C.P. 44270
Guadalajara, Jalisco, México

AVISO DE PRIVACIDAD CORTO

El **Museo Trompo Mágico**, órgano desconcentrado del **Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco (DIF Jalisco)**, con domicilio en Avenida Central número 750, Fraccionamiento Residencial Poniente, C.P. 45136, Zapopan, Jalisco, hace de su conocimiento que se considerará como datos personales a la información concerniente a una persona física identificada o identificable, y por datos personales sensibles, aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste; datos que podrán ser sometidos a tratamiento única y exclusivamente para los fines que fueron proporcionados, de acuerdo a las finalidades y atribuciones establecidas en el numeral 16 párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, así como lo dispuesto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

Los titulares de los datos personales tienen el derecho de conocer sobre el tratamiento que se les dará a los datos proporcionados al **Museo**, mediante los Avisos de Privacidad que se encuentran en cada uno de los accesos de los inmuebles de la Institución y a través de medios electrónicos por los que se recaban datos personales, a fin de tomar decisiones informadas al respecto.

El aviso de privacidad en sus modalidades: integral, simplificado y corto están disponibles para su libre acceso y consulta en nuestro Portal de Transparencia en su Artículo 8, Fracciones VIII y IX, https://transparencia.info.jalisco.gob.mx/transparencia/informacion-fundamental/12337.

Fecha de Actualización: *Noviembre de 2019.*

AVISO DE SIMPLIFICADO

El **Museo Trompo Mágico**, órgano desconcentrado del **Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco (DIF Jalisco)**, con domicilio en Avenida Central número 750, Fraccionamiento Residencial Poniente. C.P. 45136 Zapopan, Jalisco, es el responsable del uso y protección de sus datos personales, y al respecto le informa lo siguiente:

Los datos personales, se refieren a la información concerniente a una persona física identificada o identificable, y por datos personales sensibles, aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste.

Los datos personales que usted proporcione al **Museo Trompo Mágico** serán única y exclusivamente utilizados para llevar a cabo los objetivos y atribuciones de este Organismo y los utilizaremos para la integración de expedientes derivados de la atención o servicios que requiera usted como usuario, dándole el tratamiento de protección, los cuales serán almacenados con las medidas de seguridad necesarias.

Con relación a la transferencia de su información los terceros receptores de los datos personales pueden ser *Autoridades Judiciales, el Agente del Ministerio Público, la Auditoría Superior del Estado con la finalidad de dar atención a los requerimientos judiciales o legales, a los Sistemas DIF Municipales del Estado de Jalisco con la finalidad de dar seguimiento a programas o servicios, el Instituto de Transparencia Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI) para cumplir con las obligaciones de transparencia, las autoridades Federales, Estatales y Municipales, siempre que los datos se utilicen para el ejercicio de sus facultades y atribuciones.*

Los datos personales recabados, podrán ser tratados sin consentimiento del titular, siempre en respeto a sus derechos; teniendo como supuestos de excepción a los principios que rigen el tratamiento de datos según lo establece el segundo párrafo del artículo 16, de la Constitución Política de los Estados Unidos Mexicanos, así como en los supuestos consagrados en artículo 75 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Jalisco.

Usted en cualquier momento puede solicitar su *Acceso, Rectificación, Cancelación, Oposición o Revocación del consentimiento*, mediante la presentación de una solicitud

(33) 3668 1600
01 800 3000 347
Av. Alcalde # 1220
Colonia Miraflores, C.P. 44270
Guadalajara, Jalisco, México

de ejercicio de *derechos ARCO*, ante la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, ubicada en Avenida Alcalde número 1220, Colonia Miraflores, Guadalajara Jalisco. por correo electrónico oficial transparencia@difjalisco.gob.mx, *teniendo un horario de 09:00 a 15:00 horas*, de igual manera está a su disposición vía internet, la Plataforma Nacional de Transparencia (PNT).

El aviso de privacidad en sus modalidades: integral, simplificado y corto están disponibles para su libre acceso y consulta en nuestro Portal de Transparencia en su Artículo 8, Fracciones VIII y IX, https://transparencia.info.jalisco.gob.mx/transparencia/informacion-fundamental/12337.

Fecha de Actualización: *Noviembre de 2019.*

AVISO DE PRIVACIDAD INTEGRAL

El **Museo Trompo Mágico**, órgano desconcentrado del **Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco (DIF Jalisco)**, con domicilio en Avenida Central número 750, Fraccionamiento Residencial Poniente, C.P. 45136, Zapopan, Jalisco, es el responsable del uso y protección de sus datos personales, y al respecto le informa lo siguiente:

Los datos personales, aquellos que se refieren a la información concerniente a una persona física identificada o que la hace identificable, así mismo son parte esencial de la identidad de un individuo, puesto que éstos permiten hacer una referencia exacta y objetiva para particularizar a una persona y hacerla sujeta de derechos y obligaciones, y por datos personales sensibles, aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste.

El tratamiento de sus datos personales se realiza con fundamento en los artículos 1, 6 apartado A, fracciones II y III, así como el 16 párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos; 4, 7 en su párrafo segundo, 9 fracción V, de la Constitución Política del Estado de Jalisco; artículo 3 fracciones II y III, 20, 21, 22, 23, 24, 25, 26, 27 y 28 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; el 15, 19, 20, 21, 22, 24 punto 1, 25, 26, 75, 85 y 86 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Jalisco; el 25 del Código de Asistencia Social del Estado de Jalisco; los artículos 20, 21, 22, 23 fracciones II y III, 24 fracciones V y 25 fracciones XV, XVII y XX, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; el artículo 17 fracciones I, III, IV, V, VII y XII, 44, 54 BIS-4, 54 BIS-5 y 56 de la Ley para los Servidores Públicos del Estado de Jalisco y sus Municipios; el 2 fracciones III; artículo 3 del decreto del Ciudadano Gobernador Constitucional del Estado de Jalisco, mediante el cual se crea el Órgano Público Desconcentrado denominado "Museo Trompo Mágico" y 53 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

identificación, localización, acreditar el cumplimiento de los criterios de elegibilidad establecidos en las reglas de operación de los diferentes programas a cargo del sistema, llevar a cabo procesos jurídicos, la contratación de servicios personales, integrar

Jalisco

expedientes del personal, comprobar el uso adecuado de los recursos de los programas asignados, estatales y federales, tener un registro de las personas atendidas, para salvaguardar la integridad y seguridad de las y los trabajadores, así como de las y los ciudadanos que ingresan a las instalaciones del organismo asistencial, los cuales pueden ser recabados de manera directa o indirecta, medios electrónicos, escrito y vía telefónica; La información que nos proporcione, estará bajo resguardo y protegida por este, dándole el tratamiento de protección de datos sensibles, los cuales serán almacenados con las medidas de seguridad necesarias.

Con relación a la transferencia de su información los terceros receptores de los datos personales pueden ser *Autoridades Judiciales, el Agente del Ministerio Público, la Auditoría Superior del Estado con la finalidad de dar atención a los requerimientos judiciales o legales, a los Sistemas DIF Municipales del Estado de Jalisco con la finalidad de dar seguimiento a programas o servicios, el Instituto de Transparencia Información Pública y Protección de Datos Personales del Estado de Jalisco (ITEI) para cumplir con las obligaciones de transparencia, las autoridades Federales, Estatales y Municipales, siempre que los datos se utilicen para el ejercicio de sus facultades y atribuciones.*

Los datos personales recabados, podrán ser tratados sin consentimiento del titular, siempre en respeto a sus derechos; teniendo como supuestos de excepción a los principios que rigen el tratamiento de datos, la seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros, según lo establece el segundo párrafo del artículo 16, de la Constitución Política de los Estados Unidos Mexicanos, así como en los supuestos consagrados en artículo 15 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Jalisco, en los casos que se requieran del consentimiento del titular que no se realizarán transferencias de datos personales.

Usted en cualquier momento puede solicitar su *Acceso, Rectificación, Cancelación, Oposición o Revocación del consentimiento*, mediante la presentación de una solicitud de ejercicio de *derechos ARCO*, ante la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, ubicada en Avenida Alcalde número 1220, Colonia Miraflores, Guadalajara Jalisco, por correo electrónico oficial transparencia@difjalisco.gob.mx, *teniendo un horario de 09:00 a 15:00 horas*, de igual manera está a su disposición vía internet, la Plataforma Nacional de Transparencia (PNT).

Cualquier cambio al presente aviso de privacidad se hará del conocimiento de los titulares de la información confidencial, a través del Portal de Transparencia en su Artículo 8, Fracciones VIII y IX, https://transparencia.info.jalisco.gob.mx/transparencia/informacion-fundamental/12337.

***Fecha de Actualización**: Noviembre de 2019.*