Versión Pública.- Se eliminaron datos personales clasificados como Confidenciales, con fundamento en el art. 03 fracciones IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios y en el quincuagésimo octavo fracción I de los LGPICR.----------

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

ACTA DE LA DÉCIMA PRIMERA 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 VEINTISIETE DE MAYO DE DOS MIL DIECINUEVE.----------

Guadalajara, Jalisco, siendo las catorce horas con treinta y seis minutos del día veintisiete de mayo 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 numero mil doscientos veinte, Colonia Miraflores de esta Ciudad, de conformidad con los artículos 24 fracción V, 27 al 30 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, así como el numeral 10 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, del mismo modo el 30 y 32 del Reglamento Interno de la Unidad de Transparencia e Información Pública del Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco, se convocó a la **Lic. Ana Lilia Mosqueda González**, en su carácter de Directora General y Presidenta del Comité de Transparencia del Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco, al **Lic. José de Jesús Segura de León**, Titular de la Unidad de Transparencia y Secretario del Comité de Transparencia y al **Mtro. Iván Valdez Rojas**, como Titular del Órgano 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.----------

Lic. Ana Lilia Mosqueda González, Presidenta 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, siendo las catorce horas con treinta y seis minutos del día veintisiete de mayo de dos mil diecinueve, vamos a dar inicio a la décima primera 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 Presidenta, buenas tardes a todos, para efectos de esta sesión hago constar que se encuentran presentes los tres miembros del Comité de Transparencia de este

Tel: 3030 3800
01 800 3000 343
Av. Alcalde # 1220,
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.----------

Presidenta del Comité: En vista de lo anterior, **declaro formalmente instalada** la Décima Primera 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 Comité: En seguida, el proyecto de orden del día que se somete a su consideración es el siguiente: ----------

Primer Punto.- Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por el C. , ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/024/2019.----------

Segundo Punto.- Analizar el Eiercicio de Derechos ARCO, de la solicitud presentada por la C. ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/025/2019.----------

Tercer Punto.- Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por la C. ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/026/2019.----------

Cuarto Punto.- Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por la C. ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/027/2019.----------

Quinto Punto.- Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por la C. ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/028/2019.----------

Sexto Punto.- Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por el C. ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/029/2019.----------

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

Séptimo Punto.- Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por el C. , ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/030/2019.----------

Octavo Punto.- Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por la C. , ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/031/2019.----------

Noveno Punto.- Proyecto de Reglamento Interno de la Unidad de Transparencia del Sistema para el Desarrollo Integral de la Familia de Jalisco.----------

Décimo 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.----------

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

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

Es todo Presidenta.----------

Presidenta 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.----------

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

Secretario del Comité: Antes de continuar con el desahogo del orden del día, me permito solicitar su anuencia, para poner a consideración de este Comité, la dispensa de la lectura de los documentos que fueron circulados previamente para entrar directamente a su consideración y, en su caso, a la votación que corresponda.----------

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

Presidenta del Comité: Señor Secretario realice la consulta sobre la dispensa que solicita.----------

Secretario del Consejo: Miembros del Comité, se consulta si se aprueba la dispensa de la lectura de los documentos previamente circulados, los que estén por la afirmativa levanten la mano. Quedó aprobada por **unanimidad** la dispensa solicitada.----------

Consejero Presidente: Señor Secretario, por favor continúe con el desahogo del orden del día.----------

Secretario del Comité: El **Primer punto** del orden del día, corresponde **Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por el C.** , **ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/024/2019.**----------

Presidenta del Comité: Gracias, con la finalidad de poder abordar este punto del orden del día, le pido al Secretario que dé cuenta de los antecedentes que versan sobre el expediente **ARCO/024/2019.**----------

Secretario del Comité: Claro que si, en primera instancia les comento que el día diez de mayo del año en curso, se presentó una solicitud de derecho ARCO, vía INFOMEX, por parte del **C.** la cual se registró con el folio interno **ARCO/024/2019,** la cual expresa en ***"...Solicito copia certificada de mi contrato y me identifico personalmente al recoger la respuesta...",*** por lo que se procedió a revisar que cumpliera con los requisitos consagrados en el artículo 51 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Jalisco y sus Municipios, por lo que al cumplir con ellos, el día quince de mayo se admitió la solicitud, y a su vez se le requirió a la Dirección de Recursos Humanos informara si contaba con la información solicitada, por lo que mediante el memorando **DRH/477/2019**, informa que si cuenta con el documento solicitado, por lo anterior señalado, se propone a los miembros de este Comité de Transparencia resolver de manera **procedente** la solicitud del documento solicitado por el **C.** , conforme a lo estipulado en los artículos 60 y 62 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco.----------

Presidenta del Comité: Gracias, está a la consideración de ustedes la propuesta del Secretario del Comité. Si no hay intervención alguna, Secretario le pido que tome la votación correspondiente.----------

Secretario del Comité: Integrantes del Comité se consulta si se aprueba declarar

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

procedente la solicitud de derecho **ARCO/024/2019**, quienes estén por la afirmativa, levanten la mano por favor, quedo aprobado por **unanimidad**.----------

Presidenta del Comité: En virtud de lo anterior se instruye al Secretario y Titular de la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, a fin de que notifique al **C.** lo resuelto por este Comité de Transparencia, así mismo, previo a la entrega, deberá realizar el pago correspondiente de las copias certificadas, de conformidad a lo establecido en la Ley Ingresos del Estado de Jalisco para el Ejercicio dos mil diecinueve, Secretario prosiga con el desahogo del orden del día.----------

Secretario del Comité: el **Segundo Punto** del Orden del Día corresponde **Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por la C. ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/025/2019.**-----

Presidenta del Comité: Gracias, Secretario haga favor de dar cuenta sobre el expediente dicho.----------

Secretario del Comité: Enseguida Presidenta, esta solicitud fue recibida el día quince de mayo del año en curso, vía fisica, de parte de la **C.** la cual se registró con el folio interno **ARCO/025/2019,** donde solicita "...***Solicito copia certificada de mi contrato donde se especifica, mi puesto, mi horario, jornada laboral, sueldo y adscripción Museo Trompo Mágico empleado ...",*** cumpliendo con los requisitos consagrados en el artículo 51 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Jalisco y sus Municipios, se admite el día veinte de mayo, por lo que se requirió a la Dirección de Recursos Humanos informara si contaba con la información solicitada, por lo que mediante el memorando **DRH/501/2019**, precisa que si cuenta con el documento solicitado, por lo anterior señalado, se propone a los miembros de este Comité de Transparencia resolver de manera **procedente** la solicitud del documento solicitado por la **C.** conforme a lo estipulado en los artículo 60 y 62 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco.----------

Presidenta del Comité: Gracias, está a la consideración de ustedes la propuesta del Secretario del Comité, si no hay intervención alguna, Secretario le pido que tome la votación correspondiente.----------

Secretario del Comité: Integrantes del Comité se consulta si se aprueba declarar

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

procedente la solicitud de derecho ARCO mencionada, quienes estén por la afirmativa, levanten la mano por favor, quedo aprobado por **unanimidad**.----------

Presidenta del Comité: En virtud de lo anterior se instruye al Secretario y Titular de la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, a fin de que notifique al **C.** o resuelto por este Comité de Transparencia, así mismo, previo a la entrega, deberá realizar el pago correspondiente de las copias certificadas, de conformidad a lo establecido en la Ley Ingresos del Estado de Jalisco para el Ejercicio dos mil diecinueve, Secretario prosiga con el desahogo del orden del día.----------

Secretario del Comité: el **Tercer Punto** del Orden del Día corresponde **Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por la C. ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/026/2019.**----------

Presidenta del Comité: Gracias, Secretario de vista del expediente en comento.---------

Secretario del Comité: Integrantes del Comité, el día quince de mayo del año en curso, se presentó una solicitud de derecho ARCO, vía física, de la **C. Patricia Santos Galván,** la cual se registró con el folio interno **ARCO/026/2019,** la cual expresa en ***"...Solicito copia certificada de mi contrato donde se especifica, mi puesto, mi horario, jornada laboral, sueldo y adscripción..." Empleado ...",*** por lo que se procedió a revisar que cumpliera con los requisitos de la Ley, por lo que al cumplir con ellos, el día veinte de mayo se admitió la solicitud, asimismo se le requirió a la Dirección de Recursos Humanos informara si contaba con la información solicitada, por lo que mediante el memorando **DRH/500/2019**, informa que si cuenta con el documento solicitado, por lo anterior señalado, se propone a los miembros de este Comité de Transparencia resolver de manera **procedente** la solicitud del documento solicitado por la **C.** conforme a lo estipulado en los numerales 60 y 62 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco.----------

Presidenta del Comité: Gracias, está a la consideración de ustedes la propuesta del Secretario del Comité. Si no hay intervención alguna, Secretario le pido que tome la votación correspondiente.----------

Secretario del Comité: Integrantes del Comité se consulta si se aprueba declarar procedente la solicitud de derecho **ARCO/026/2019**, quienes estén por la afirmativa, levanten la mano por favor, quedo aprobado por **unanimidad**.----------

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

Presidenta del Comité: En virtud de lo anterior se instruye al Secretario y Titular de la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, a fin de que notifique al **C.** lo resuelto por este Comité de Transparencia, y realice las gestiones necesarias para la entrega de los documentos solicitados, previo a la entrega, se deberá realizar el pago correspondiente de las copias certificadas, de conformidad a lo establecido en la Ley Ingresos del Estado de Jalisco para el Ejercicio dos mil diecinueve, Secretario prosiga con el desahogo del orden del día.----------

Secretario del Comité: el **Cuarto Punto** del Orden del Día corresponde **Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por la C. ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/027/2019.**-----

Presidenta del Comité: Gracias, Secretario haga favor de dar cuenta sobre el expediente dicho.----------

Secretario del Comité: Enseguida Presidenta, esta solicitud fue recibida el día quince de mayo del año en curso, vía física, de parte de la **C.** , la cual se registró con el folio interno **ARCO/027/2019,** donde solicita ***"...Copia de contrato certificado (*** ***)..."***, cumpliendo con los requisitos de Ley, se admite el día veinte de mayo, del mismo modo se le requirió a la Dirección de Recursos Humanos informara si contaba con la información solicitada, por lo que mediante el memorando **DRH/498/2019**, precisa que si cuenta con el documento solicitado, por lo anterior señalado, se propone a los miembros de este Comité de Transparencia resolver de manera **procedente** la solicitud del documento solicitado por la **C.** , conforme a lo estipulado en los artículo 60 y 62 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco.----------

Presidenta del Comité: Gracias, está a la consideración de ustedes la propuesta del Secretario del Comité, si no hay intervención alguna, Secretario le pido que tome la votación correspondiente.----------

Secretario del Comité: Integrantes del Comité se consulta si se aprueba declarar procedente la solicitud de derecho **ARCO/027/2019**, quienes estén por la afirmativa, levanten la mano por favor, quedo aprobado por **unanimidad**.----------

Presidenta del Comité: En virtud de lo anterior se instruye al Secretario y Titular de la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, a

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

fin de que notifique al **C.** lo resuelto por este Comité de Transparencia, así mismo, previo a la entrega, deberá realizar el pago correspondiente de las copias certificadas, de conformidad a la Ley Ingresos del Estado de Jalisco para el Ejercicio dos mil diecinueve, Secretario prosiga con el desahogo del orden del día.----

Secretario del Comité: el **Quinto Punto** del Orden del Día corresponde **Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por la C. ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/028/2019.**-----

Presidenta del Comité: Gracias, Secretario de vista del expediente **ARCO/028/2019.**--

Secretario del Comité: Integrantes del Comité, el día quince de mayo del año en curso, se presentó una solicitud de derecho ARCO, vía INFOMEX, de la **C.** la cual se registró con el folio interno **ARCO/028/2019,** la cual expresa en ***"...Solicito copia certificada de mi contrato laboral y me identifico al recoger la respuesta personalmente..."***, por lo que se procedió a revisar que cumpliera con los requisitos de la Ley, por lo que al cumplir con ellos, el día veinte de mayo se admitió la solicitud, se le requirió a la Dirección de Recursos Humanos informara si contaba con la información solicitada, por lo que mediante el memorando **DRH/502/2019**, informa que si cuenta con el documento solicitado, por lo anterior señalado, se propone a los miembros de este Comité de Transparencia resolver de manera **procedente** la solicitud del documento solicitado por la **C.** , conforme a lo estipulado en los artículos 60 y 62 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco.----------

Presidenta del Comité: Gracias, está a la consideración de ustedes la propuesta del Secretario del Comité, si no hay intervención alguna, Secretario le pido que tome la votación correspondiente.----------

Secretario del Comité: Integrantes del Comité se consulta si se aprueba declarar procedente la solicitud de derecho **ARCO/028/2019**, quienes estén por la afirmativa, levanten la mano por favor, quedo aprobado por **unanimidad**.----------

Presidenta del Comité: En virtud de lo anterior se instruye al Secretario y Titular de la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, a fin de que notifique al **C.** lo resuelto por este Comité de Transparencia, y realice las gestiones necesarias para la entrega del documento solicitado, así mismo, previo a la entrega, deberá realizar el pago correspondiente de

las copias certificadas, de conformidad a la Ley Ingresos del Estado de Jalisco para el Ejercicio dos mil diecinueve, Secretario prosiga con el desahogo del orden del día.-------

Secretario del Comité: el **Sexto Punto** del Orden del Día corresponde **Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por el C.** **ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/029/2019.**----------

Presidenta del Comité: Gracias, Secretario haga favor de dar cuenta sobre dicho expediente.----------

Secretario del Comité: Enseguida Presidenta, esta solicitud fue recibida el día diecisiete de mayo del año en curso, vía física, de parte del **C.** la cual se registró con el folio interno **ARCO/029/2019,** donde solicita ***"...Solicito copia certificada de mi contrato laboral ultimo firmado. Museo Trompo Magico...",*** cumpliendo con los requisitos consagrados en el artículo 51 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Jalisco y sus Municipios, se admite el día veintiuno de mayo, se requirió a la Dirección de Recursos Humanos informara si contaba con la información solicitada, por lo que mediante el memorando **DRH/499/2019**, precisa que si cuenta con el documento solicitado, por lo anterior señalado, se propone a los miembros de este Comité de Transparencia resolver de manera **procedente** la solicitud de los documentos solicitado por el **C.** conforme a lo estipulado en los numerales 60 y 62 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco.----------

Presidenta del Comité: Gracias, está a la consideración de ustedes la propuesta del Secretario del Comité. Si no hay intervención alguna, Secretario le pido que tome la votación correspondiente.----------

Secretario del Comité: Integrantes del Comité se consulta si se aprueba declarar procedente la solicitud de derecho ARCO, quienes estén por la afirmativa, levanten la mano por favor, quedo aprobado por **unanimidad**.----------

Presidenta del Comité: En virtud de lo anterior se instruye al Secretario y Titular de la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, a fin de que notifique al **C.** lo resuelto por este Comité de Transparencia, así mismo, previo a la entrega, deberá realizar el pago correspondiente de las copias certificadas, de conformidad a la Ley Ingresos del Estado de Jalisco para el Ejercicio dos mil diecinueve, Secretario prosiga con el desahogo del orden del día.----

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

Secretario del Comité: El **Séptimo punto** del orden del día, corresponde **Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por el C.** , **ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/030/2019.**----------

Presidenta del Comité: Gracias, Secretario que dé cuenta de los antecedentes que versan sobre el expediente **ARCO/030/2019**.----------

Secretario del Comité: Claro que si, en primera instancia les comento que el día diecisiete de mayo del año en curso, se presentó una solicitud de derecho ARCO, vía física, por parte del **C.** la cual se registró con el folio interno **ARCO/030/2019,** la cual expresa en ***"...Solicito copia certificada de mi contrato laboral ultimo firmado. No. empleado en Trompo Mágico..."***, por lo que se procedió a revisar que cumpliera con los requisitos consagrados en el artículo 51 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Jalisco y sus Municipios, por lo que al cumplir con ellos, el día veintidós de mayo se admitió la solicitud, asimismo se le requirió a la Dirección de Recursos Humanos informara si contaba con la información solicitada, por lo que mediante el memorando **DRH/510/2019**, informa que si cuenta con el documento solicitado, por lo anterior señalado, se propone a los miembros de este Comité de Transparencia resolver de manera **procedente** la solicitud del documento solicitado por el **C.** conforme a lo estipulado en los artículo 60 y 62 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco.----------

Presidenta del Comité: Gracias, está a la consideración de ustedes la propuesta del Secretario del Comité, si no hay intervención alguna, Secretario le pido que tome la votación correspondiente.----------

Secretario del Comité: Integrantes del Comité se consulta si se aprueba declarar procedente la solicitud de derecho **ARCO/030/2019**, quienes estén por la afirmativa, levanten la mano por favor, quedo aprobado por **unanimidad**.----------

Presidenta del Comité: En virtud de lo anterior se instruye al Secretario y Titular de la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, a fin de que notifique al **C.** lo resuelto por este Comité de Transparencia, así mismo, previo a la entrega, deberá realizar el pago correspondiente de las copias certificadas, de conformidad a lo establecido en la Ley Ingresos del Estado de Jalisco para el Ejercicio dos mil diecinueve, Secretario prosiga con el desahogo del orden del día.----------

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

Secretario del Comité: el **Octavo Punto** del Orden del Día corresponde **Analizar el Ejercicio de Derechos ARCO, de la solicitud presentada por la C.** , **ante el Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco; asignándole el número expediente interno ARCO/031/2019.**-----

Presidenta del Comité: Gracias, Secretario haga favor de dar cuenta sobre dicho expediente.----------

Secretario del Comité: Enseguida Presidenta, esta solicitud fue recibida el día diecisiete de mayo del año en curso, vía INFOMEX, de parte de la **C.** la cual se registró con el folio interno **ARCO/031/2019,** donde solicita ***"...Solicito copia certificada de mi ultimo contrato laboral. Me identifico al recogerlo personalmente..."***, cumpliendo con los requisitos consagrados en el artículo 51 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Jalisco y sus Municipios, se admite el día veintiuno de mayo, se requirió a la Dirección de Recursos Humanos informara si contaba con la información solicitada, por lo que mediante el memorando **DRH/497/2019**, precisa que si cuenta con el documento solicitado, por lo anterior señalado, se propone a los miembros de este Comité de Transparencia resolver de manera **procedente** la solicitud de los documentos solicitado por la **C.** , conforme a lo estipulado en los numerales 60 y 62 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco.----------

Presidenta del Comité: Gracias, está a la consideración de ustedes la propuesta del Secretario del Comité, si no hay intervención alguna, Secretario le pido que tome la votación correspondiente.----------

Secretario del Comité: Integrantes del Comité se consulta si se aprueba declarar procedente la solicitud de derecho ARCO, quienes estén por la afirmativa, levanten la mano por favor, quedo aprobado por **unanimidad**.----------

Presidenta del Comité: En virtud de lo anterior se instruye al Secretario y Titular de la Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados, a fin de que notifique al **C.** o resuelto por este Comité de Transparencia, así mismo, previo a la entrega, deberá realizar el pago correspondiente de las copias certificadas, de conformidad a la Ley Ingresos del Estado de Jalisco para el Ejercicio dos mil diecinueve, Secretario prosiga con el desahogo del orden del día.----------

Secretario del Comité: El **Noveno Punto** del Orden del Día corresponde en el

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

Proyecto de Reglamento Interno de la Unidad de Transparencia del Sistema para el Desarrollo Integral de la Familia de Jalisco.----------

Presidenta del Comité: Integrantes del Comité, está a la consideración de ustedes el proyecto de Reglamento anteriormente referido, en virtud de la publicación del Estatuto Orgánico de esta Institución, en el Periódico Oficial "El Estado de Jalisco" el día veintiuno del presente mes y año, se tuvo que adecuar el reglamento interno en materia de transparencia, para que coincidiera con la realidad jurídica del Sistema para el Desarrollo Integral de la Familia de Jalisco. 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 Reglamento citado, quienes estén por la afirmativa, levanten la mano por favor, quedo aprobado por **unanimidad** el Reglamento mencionado.----------

Presidenta del Comité: Gracias Secretario prosiga con el desahogo del orden del día.-

Secretario del Comité: El **Décimo Punto** del Orden del Día corresponde en el **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.**----------

Presidenta 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, al igual que en el reglamento de transparencia, por la publicación del Estatuto Orgánico, se tuvo que modificar el documento de seguridad, afín de que correspondiera con la nueva estructura aprobada. .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.----------

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

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

Presidenta del Comité: Integrantes del Comité, está a la consideración de ustedes los

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

Proyectos de los Avisos de Privacidad del Sistema DIF Jalisco y sus Órganos Desconcentrados, para que queden acorde a las funciones establecidas en el Código de Asistencia Social del estado de Jalisco y el Estatuto Orgánico de la Institución. 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**.----------

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

Secretario del Comité: El **Décimo Segundo 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**.----------

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

Presidenta del Comité: Gracias Secretario, agradezco a todos su presencia a esta sesión, siendo las quince horas con veinte minutos del día veintisiete de mayo del dos mil diecinueve, se da por concluida la décima primera sesión extraordinaria del Comité de Transparencia.----------

Se levanta la presente acta que consta de catorce 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. ----------

Lic. Ana Lilia Mosqueda González
Presidenta del Comité de Transparencia

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

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

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

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 veintisiete de mayo 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 catorce fojas y sus anexos. **CONSTE.**----------

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

REGLAMENTO INTERNO DE LA UNIDAD DE TRANSPARENCIA DEL SISTEMA PARA EL DESARROLLO INTEGRAL DE LA FAMILIA DE JALISCO

TÍTULO PRIMERO
Disposiciones Generales

CAPÍTULO ÚNICO

Artículo 1.- El presente Reglamento es de orden público, de observancia general y obligatoria para el Sistema para el Desarrollo Integral de la Familia de Jalisco, de conformidad con lo establecido en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, atendiendo a garantizar el derecho fundamental de toda persona para conocer el proceso y la toma de decisiones públicas, así como para solicitar, acceder, consultar, recibir, difundir, reproducir y publicar la información pública en posesión de los sujetos obligados.

Artículo 2.- Este reglamento se expide con fundamento en lo dispuesto por los artículos en la Constitución Política de los Estados Unidos Mexicanos; la Constitución Política del Estado de Jalisco; la Ley Orgánica del Poder Ejecutivo del Estado de Jalisco; así como lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública y la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios y en el Estatuto Orgánico del Sistema para el Desarrollo Integral de la Familia de Jalisco.

Artículo 3.- Para los efectos de este Reglamento se entenderá por:

I. **Comité:** El Comité de Transparencia del Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco;

II. **Enlace de Transparencia:** Servidor público responsable de gestionar la información pública al interior de la dependencia de la Unidad Administrativa a la que se encuentra adscrito, tanto en lo relativo a las solicitudes de acceso a la información pública, obligaciones en materia de transparencia y protección de datos personales;

III. **Información pública:** Toda información que generen, posean o administren los sujetos obligados, como consecuencia del ejercicio de sus facultades o atribuciones, o el cumplimiento de sus obligaciones, sin importar su origen, utilización o el medio en el que se contenga o almacene; la cual está contenida en documentos, fotografías, grabaciones, soporte magnético, digital, sonoro, visual, electrónico, informático, holográfico o en cualquier otro elemento técnico existente o que surja

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

con posterioridad;

IV. **Instituto**: El Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco;

V. **Ley:** La Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios;

VI. **Ley General:** Ley General de Transparencia y Acceso a la Información Pública;

VII. **Lineamientos:** Los Lineamientos Generales para la Protección de la Información Confidencial y Reservada que deberán observar los Sujetos Obligados previsto en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, expedidas por el Instituto;

VIII. **Plataforma Nacional de Transparencia:** Plataforma electrónica para el cumplimiento de los procedimientos, obligaciones y disposiciones en materia de transparencia, acceso a la información y protección de datos personales e información confidencial, conformada con al menos los sistemas de solicitudes de información, gestión de medios de impugnación, sitios de Internet para la publicación de obligaciones de transparencia y sistemas de comunicación con Organismos Garantes y Sujetos Obligados;

IX. **Portal:** Portal de Internet que contiene la Información Fundamental de un Sujeto Obligado.

X. **Sistema DIF Jalisco**: Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco;

XI. **Solicitante:** Persona ya sea física o jurídica, que ingresa una solicitud de Información en términos de lo establecido por la Ley;

XII. **Solicitud:** A aquella solicitud de información que reúne los requisitos previstos en la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios;

XIII. **Unidad Administrativa:** Sujeto responsable dentro de un sujeto obligado que, en el marco de sus atribuciones y facultades, genera, posee o administra información pública; y

XIV. **UTIDIF:** La Unidad de Transparencia del Sistema para el Desarrollo Integral de la Familia del Estado de Jalisco.

Artículo 4.- Es de aplicación supletoria para este Reglamento, lo establecido en:

I. La Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; y

II. La Ley General de Transparencia y Acceso a la Información Pública.

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

TÍTULO SEGUNDO
De los Sujetos Obligados

Capítulo I
Disposiciones Generales

Artículo 5.- Para efectos de este Reglamento, son Sujetos Obligados los que se señalan en el artículo 24 de la Ley y los que así designe el Instituto con ese carácter.

Artículo 6.- Son obligaciones de los Sujetos Obligados, además de las establecidas en el artículo 25 de la Ley, las siguientes:

I. Atender lo establecido en la Ley, los lineamientos del Sistema Nacional, lineamientos del Instituto, y los que determine el Comité y la Junta de Gobierno del Sistema DIF Jalisco;
II. Observar los principios rectores establecidos en el artículo 5 de la Ley, en la interpretación y aplicación del Reglamento;
III. Promover acuerdos con instituciones públicas especializadas que puedan colaborar en la traducción de información pública fundamental y atención de solicitudes de información en la lengua indígena que se requiera; y
IV. Presentar la denuncia penal respectiva a través de su representante legal, por pérdida, extravío, robo o destrucción indebida de la información, aportando los elementos de prueba para tales efectos, con base en la investigación que abra para ello el Órgano Interno de Control.

Artículo 7.- Son Unidades Administrativa:

I. Dirección General;
II. Órgano Interno de Control;
III. Dirección Jurídica;
IV. Dirección de Control de la Gestión Institucional;
V. Subdirección General Operativa;
VI. Dirección de Atención a Personas con Discapacidad;
VII. Dirección de Atención a las Personas Adultas Mayores;
VIII. Dirección de Atención a la Infancia;
IX. Dirección de Trabajo Social;
X. Dirección de Atención a Personas en Situación de Emergencia;
XI. Procuraduría de Protección de Niñas, Niños y Adolescentes del Estado de Jalisco;
XII. Subdirección General de Seguridad Alimentaria;

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

XIII. Dirección de Comedores y Centros de Distribución de Alimentos;
XIV. Subdirección General de Desarrollo Comunitario y Apoyo Municipal;
XV. Dirección de Vinculación Municipal;
XVI. Subdirección General Administrativa;
XVII. Dirección de Planeación Institucional;
XVIII. Dirección de Tecnologías y Sistemas Informáticos;
XIX. Dirección de Recursos Humanos;
XX. Dirección de Recursos Financieros;
XXI. Dirección de Recursos Materiales;
XXII. Dirección de Servicios Generales; y
XXIII. Dirección General Museo Trompo Mágico;

Artículo 8.- Son obligaciones de las Unidades Administrativas:

I. Incorporarse a la Plataforma Nacional a través de la UTIDIF, con base en las disposiciones de la Ley General de Transparencia, los lineamientos que emita el Sistema Nacional y las que establezca el Instituto;
II. Designar a un Enlace de Transparencia de su área ante la UTIDIF, que administre la cuenta de usuario para la Plataforma Nacional que se le asigne;
III. Orientar y apoyar a los solicitantes de información para garantizar el ejercicio de los derechos de acceso a la información y protección de datos personales;
IV. Brindar a las personas con discapacidad o que hablen lenguas indígenas, las facilidades y apoyos necesarios para el ejercicio del derecho de acceso a la información y protección de datos personales, con base en los acuerdos que establezca el Sujeto Obligado con base en lo establecido en las fracción III del artículo 6 del Reglamento;
V. Atender lo establecido en la Ley, los lineamientos del Sistema Nacional, lineamientos del Instituto, y los que determine el Comité y la Junta de Gobierno del Sistema DIF Jalisco;
VI. Proporcionar la Información Fundamental, Proactiva o Focalizada, bajo los principios que establezca la Ley y Lineamientos emitidos por el Instituto y el Sistema Nacional, que le sea requerida por la UTIDIF, para ser publicada en Internet y por medios de fácil acceso;
VII. Proporcionar la información pública de libre acceso que le requiera la UTIDIF, con base en solicitudes de información presentadas;
VIII. Enviar al Comité sus consideraciones, fundadas y motivadas, de clasificación inicial de información pública de libre acceso sobre cada solicitud de información que le requiera la UTIDIF, atendiendo a lo dispuesto en la Ley;

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

IX. Enviar a la UTIDIF sus propuestas de clasificación y protección de información confidencial sobre la información requerida mediante solicitud de información;

X. Promover la capacitación y cultura de la transparencia, acceso a la información, rendición de cuentas y combate a la corrupción, entre las áreas a su cargo, en coordinación con la UTIDIF; y

XI. Hacer del conocimiento del Comité y al Órgano Interno de Control la inexistencia de información por pérdida, extravío, robo o destrucción indebida de la información, y proveer a dichas instancias de los elementos necesarios para desahogar las diligencias que de ello se deriven.

Para el cumplimiento de lo establecido en la fracción IV los Sujetos Obligados promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a entregar las repuestas a solicitudes de información, en la lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente.

CAPÍTULO II
Del Comité de Transparencia

Artículo 9.- El Sistema DIF Jalisco contará con un Comité de Transparencia con base en las disposiciones de la Ley y del presente Reglamento.

Artículo 10.- El Comité de Transparencia es el órgano interno del Sistema DIF Jalisco, encargado de la clasificación de la información pública.

Artículo 11.- El Comité estará integrado por:

I. Un Presidente del Comité, quien será el Director General del Sistema DIF Jalisco o quien tenga a bien en designar para delegarle tal representatividad, conforme a lo consagrado en la Ley;

II. Un Secretario del Comité, el Titular de la UTIDIF; y

III. Un Vocal, El Titular del Órgano Interno de Control.

Los integrantes del Comité de Transparencia no podrán depender jerárquicamente entre sí, tampoco podrán reunirse dos o más de estos integrantes en una sola persona.

Artículo 12.- En el supuesto de sustitución de alguno de sus integrantes, sea por cambio, remoción, renuncia o separación del cargo, el Titular de la UTIDIF notificará al Instituto en los siguientes cinco días hábiles la sustitución.

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

Artículo 13.- Los funcionarios que no sean integrantes del Comité, podrán participar en sus sesiones atendiendo lo siguiente:

I. Los Titulares de las Unidades Administrativas que soliciten participar en alguna sesión, por sí o algún representante, lo podrán hacer cuando estas versen sobre asuntos de su competencia;

II. El Secretario del Comité podrá invitar a los titulares de las Unidades Administrativas, o a quien estos determinen, para participar en las sesiones cuando se requiera información adicional para los procesos deliberativos de clasificación o desclasificación de información pública, clasificación y protección de información confidencial, así como declaratoria de inexistencia; y

III. Los servidores públicos que no sean parte del Comité sólo tendrán derecho a voz.

Artículo 14.- El Comité tendrá las siguientes atribuciones:

I. Instituir, coordinar y supervisar, en términos de las disposiciones aplicables, las acciones y los procedimientos para asegurar la mayor eficacia en la gestión de las solicitudes en materia de acceso a la información y el ejercicio de los derechos ARCO;

II. Confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas del Sistema DIF Jalisco , en materia de acceso a la información o el ejercicio de derechos ARCO;

III. Ordenar, en su caso, a las áreas competentes, que generen la información que derivado de sus facultades, competencias y funciones deban tener en posesión o que, previa acreditación de la imposibilidad de su generación, exponga, de forma fundada y motivada, las razones por las cuales no ejercieron dichas facultades, competencias o funciones, lo anterior de conformidad con su normativa interna;

IV. Resolver en todas las solicitudes de ejercicio de derechos ARCO que le presenten, pudiendo delegar a la UTIDIF los casos en que esta puede resolver;

V. Establecer políticas para facilitar la obtención de información y el ejercicio del derecho de acceso a la información;

VI. Promover la capacitación y actualización de los servidores públicos y de los integrantes adscritos a la UTIDIF;

VII. Establecer programas de capacitación en materia de transparencia, acceso a la información, accesibilidad y protección de datos personales, para todos los servidores públicos o integrantes del Sistema DIF Jalisco ;

VIII. Solicitar y autorizar la ampliación del plazo de reserva de la información, de

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

conformidad con las disposiciones aplicables en la materia;

IX. Revisar que los datos de la información confidencial que reciba sean exactos y actualizados;

X. Registrar y controlar la transmisión a terceros, de información reservada o confidencial en su poder;

XI. Establecer un índice de la información clasificada como confidencial o reservada; y

XII. Las demás que establezcan otras disposiciones legales y reglamentarias aplicables

Artículo 15.- El Comité sesionará de manera ordinaria una vez cada cuatro meses y de manera extraordinaria cuantas veces estime necesario.

Artículo 16.- La convocatoria para las sesiones del Comité se hará con dos días de anticipación tratándose de sesiones ordinarias, y con veinticuatro horas de anticipación para las sesiones extraordinarias. La convocatoria deberá contener el orden el día a tratar.

En caso de urgencia, se podrá dispensar el término para convocar, y en el acta de la sesión se deberán incluir los asuntos desahogados.

Artículo 17.- Para que tengan validez las sesiones del Comité, se requerirá la asistencia de cuando menos dos de sus integrantes para sesionar y sus decisiones se toman por mayoría simple de votos.

Artículo 18.- El Presidente del Comité tiene las siguientes facultades y obligaciones:

I. Presidir las sesiones;

II. Tener voto de calidad en caso de empate;

III. Otorgar las condiciones necesarias para el buen funcionamiento del Comité; y

IV. Aquéllas que por la naturaleza del cargo le correspondan.

Artículo 19.- El Secretario tendrá las siguientes facultades y obligaciones:

I. Convocar para las sesiones;

II. Redactar las actas de las sesiones;

III. Proponer los proyectos de acuerdos y actas de clasificación de información y sesiones restringidas;

IV. Dar seguimiento a los acuerdos;

V. Supervisar la ejecución del programa de trabajo y de la estrategia en todas las áreas;

VI. Llevar el archivo del Comité; y

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

VII. Aquéllas que por la naturaleza del cargo le correspondan.

Al concluir cada sesión levantará un acta con los puntos que se trataron en la misma y de los acuerdos tomados; el acta deberá ser firmada por todos los que participaron en la sesión.

CAPÍTULO III
De la Unidad de Transparencia (UTIDIF)

Artículo 20.- La UTIDIF es la Unidad de Transparencia del Sistema DIF Jalisco, que tiene bajo su encargo la recepción, trámite y entrega de información respecto de las solicitudes presentadas conforme a la Ley y demás normativa vinculada con dicho derecho fundamental.

Artículo 21.- La UTIDIF realizará todas las acciones tendientes a atender solicitudes de información, darle trámite y seguimiento a las mismas, así como asesorar y auxiliar a los solicitantes y garantizar el derecho fundamental de toda persona para tener acceso a la información pública que se genera como sujeto obligado.

Artículo 22.- La UTIDIF tendrá las siguientes atribuciones:

I. Administrar el Portal del Sujeto Obligado;
II. Actualizar mensualmente la información fundamental;
III. Recibir y dar respuesta a las solicitudes de información pública y de derechos ARCO, para lo cual debe integrar el expediente, realizar los trámites internos y desahogar el procedimiento respectivo;
IV. Tener a disposición del público formatos para presentar solicitudes de información pública y derecho ARCO;
V. Llevar el registro y estadística de las solicitudes de información pública y realizar la captura dentro del Sistema SIRES;
VI. Asesorar gratuitamente a los solicitantes en los trámites para acceder a la información pública;
VII. Asistir gratuitamente a los solicitantes que lo requieran para elaborar una solicitud de información pública;
VIII. Requerir y recabar de las oficinas correspondientes la información pública de las solicitudes procedentes;
IX. Solicitar al Comité de Transparencia interpretación o modificación de la clasificación de información pública solicitada;
X. Capacitar al personal del Organismo para dar de manera eficiente respuestas a las solicitudes de información;
XI. Informar a Dirección General y al Instituto sobre la negativa de las Unidades

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

Administrativas para entregar información pública de libre acceso;

XII. Proponer al Comité de Transparencia procedimientos internos que aseguren la mayor eficiencia en la gestión de las solicitudes de acceso a la información y Derecho ARCO;

XIII. Coadyuvar en la promoción de la cultura de la transparencia y el acceso a la información pública; y

XIV. Las demás que establezcan otras disposiciones legales o reglamentarias aplicables.

Artículo 23.- La UTIDIF dispondrá de los elementos humanos, así como de los recursos materiales y técnicos que sean necesarios para el desempeño de sus actividades y, que para ello, le sean asignados por las instancias administrativas del Sistema DIF Jalisco.

TITULO TERCERO
De los Tipos de Información

CAPÍTULO ÚNICO
De la Información Pública

Artículo 24.- Por regla general, toda la información que genere el Sistema DIF Jalisco, es de libre acceso, salvo aquélla que se clasifique como reservada o confidencial de acuerdo a lo previsto por los artículos 17 y 20 de la Ley.

Artículo 25.- El Sistema DIF Jalisco, a través de la UTIDIF, está obligado a recabar, reproducir, publicar y difundir toda la información fundamental a que se refiere el artículo 8 de la Ley.

La información pública fundamental que genere el Sistema DIF Jalisco, deberá publicarse por los medios electrónicos de que disponga, por los medios establecidos en la Ley. Conforme a su presupuesto, se deberán instalar equipos informáticos con acceso a Internet para que los solicitantes puedan consultar, por ese medio, la información fundamental que genere el Sistema DIF Jalisco.

Artículo 26.- La Información Pública Protegida es la información cuyo acceso es restringido y se divide en Información pública confidencial e Información pública reservada.

Artículo 27.- La Información Pública Confidencial, es la información pública protegida, intransferible e indelegable, relativa a los particulares, que por disposición legal queda prohibido su acceso, distribución, comercialización, publicación y difusión generales de forma

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

permanente, con excepción de las autoridades competentes que, conforme a esta ley o la legislación estatal en materia de protección de datos personales en posesión de sujetos obligados, tengan acceso a ella, y de los particulares titulares de dicha información.

La Información Pública Reservada, es la información pública protegida, relativa a la función pública, que por disposición legal temporalmente queda prohibido su manejo, distribución, publicación y difusión generales, con excepción de las autoridades competentes que, de conformidad con la ley, tengan acceso a ella.

Artículo 28.- En la Clasificación de Información Pública como Reservada, se observará el siguiente procedimiento:

I. La Unidad Administrativa, al recibir una solicitud de información que presuma estar sujeta a ser reservada, en los primeros dos días hábiles posteriores a su recepción propondrá una reserva inicial, para lo que aportará y propondrá a la UTIDIF elementos que la motiven y la justifiquen observando lo siguiente:

- **a)** El catálogo, las excepciones, la negación, periodos y extinción de reserva establecido en la Ley;
- **b)** Los lineamientos emitidos por el Instituto; y
- **c)** La vigencia de las excepciones, la negación, periodos y extinción de reserva establecida en la Ley, con base en antecedentes de reserva aplicados a casos iguales.

II. El Comité, con la propuesta de reserva inicial, analizará y determinará la clasificación total o parcial de la información requerida, asentándose en un acta;

III. La resolución del Comité sobre la clasificación de información podrá ser:

a) Total; o
b) Parcial.

IV. En el caso que la clasificación sea parcial, el Comité, con el apoyo de la Unidad Administrativa, elaborará una versión pública del documento con la información requerida y clasificada, la cual se integrará al expediente de clasificación; y

V. La UTIDIF notificará al solicitante la resolución del Comité e inscribirá la resolución en el índice de información clasificada, y en su caso entregará la versión pública.

Artículo 29.- En la Clasificación de Información Confidencial, se observará el siguiente procedimiento:

I. La Unidad Administrativa, al recibir de la Unidad una solicitud de información que presuma contiene elementos sujetos a reserva y protección por contener datos personales y ser confidencial, en los primeros dos días hábiles posteriores a su

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

recepción aportará lo necesario para fundarlo y motivarlo, y lo propondrá a la UTIDIF, con base en lo establecido en la Ley, y los lineamientos emitidos por el Instituto;

II. La Unidad Administrativa, en su propuesta de reserva y protección de información confidencial, deberá incluir de manera precisa y clara los motivos y fundamentos legales, sobre las reservas de cada uno de los datos;

III. La Unidad Administrativa elaborará una versión pública del documento con la información requerida, testando los datos personales e indicando en el mismo y al margen del documento el fundamento legal, la cual enviará a la UTIDIF; y

IV. La UTIDIF validará la versión pública y la entregará al solicitante.

Artículo 30.- Para la Protección de Datos Personales e Información Confidencial, se observará lo siguiente:

I. Toda persona, titular de datos personales e información confidencial, puede solicitar ante el sujeto obligado en cualquier tiempo el acceso, rectificación, cancelación y oposición;

II. Para el ejercicio del derecho anterior, se procederá conforme a lo establecido en las disposiciones legales en la materia;

III. La Unidad Administrativa, que requieran y soliciten a particulares de información datos personales para el ejercicio de sus atribuciones, sujeta a protección con base en la normatividad aplicable, deberán tomar las medidas de seguridad necesarias para su resguardo, así como uso distinto para la que fue requerida;

IV. La Unidad Administrativa, exhibirán en un lugar público el Aviso de Privacidad respectivo y notificarán a la UTIDIF las bases de datos que elaboren con la información recabada, observando las disposiciones legales en la materia y los lineamientos emitidos al respecto por parte del Instituto; y

V. La Unidad Administrativa, al recibir de la UTIDIF una solicitud de ejercicio de derechos de acceso, rectificación, cancelación y oposición, así como Protección de Información Confidencial, le informará sobre su existencia y procedencia; asimismo, aportará los elementos existentes para que el Comité determine el sentido de la respuesta que se le dará a través de la UTIDIF al solicitante, conforme a lo establecido en la Ley.

TITULO CUARTO
Del Proceso de Acceso a la Información

CAPÍTULO I

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

De las Solicitudes de Acceso a la Información Pública

Artículo 31.- Las solicitudes de información pública al Sistema DIF Jalisco, podrán formularse mediante escrito libre o en los formatos que para tal efecto determine la UTIDIF, a través del correo electrónico, por comparecencia, vía telefónica, de igual manera, podrá hacer la correspondiente solicitud de información a través del sistema INFOMEX.

Las solicitudes de acceso a la información serán recibidas por la UTIDIF, en días y horas hábiles, para darle trámite y debida substanciación, en caso de que una solicitud sea ingresada en días y horas inhábiles para el Sistema DIF Jalisco, la misma se le tendrá como recibida al día hábil siguiente.

Artículo 32.- La solicitud de información podrá presentarse por cualquier persona física, sin necesidad de acreditar personalidad o identidad, salvo en el caso de las peticiones de acceso o corrección de datos personales o información confidencial. Tratándose de personas jurídicas, la solicitud debe presentarse a través de su representante legal.

Artículo 33.- En caso de que el solicitante no sepa leer o escribir o se encuentre imposibilitado por cualquier otro motivo, el personal de la UTIDIF auxiliará al solicitante en el llenado de la petición de acceso a la información, debiendo leerlo en voz alta al peticionario y en caso de estar de acuerdo, estampará su firma o huella digital.

Artículo 34.- Los requisitos mínimos que debe contener una solicitud de información son:

- **I.** Nombre del sujeto obligado a quien se dirige;
- **II.** Nombre del solicitante o seudónimo y autorizados para recibir la información, en su caso;
- **III.** Domicilio, número de fax, correo electrónico o los estrados de la UTIDIF, para recibir notificaciones, e
- **IV.** Información solicitada, incluida la forma y medio de acceso de la misma, la cual estará sujeta a la posibilidad y disponibilidad que resuelva el sujeto obligado.

La información de la fracción II del presente artículo será proporcionada por el solicitante de manera opcional y, en ningún caso, podrá ser un requisito indispensable para la procedencia de la solicitud.

Artículo 35.- En caso de que la solicitud de información no reúna los requisitos previstos por el artículo anterior, la UTIDIF prevendrá directamente al solicitante conforme a lo previsto en el

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

artículo 82 de la Ley, dentro de los dos días hábiles siguientes a la presentación de la solicitud, con la finalidad de que lo subsane su solicitud, so pena de tener por no presentada la solicitud.

Artículo 36.- Cuando se presente una solicitud de acceso a la información pública donde otro Sujeto Obligado le corresponda atender, la UTIDIF deberá remitir al sujeto obligado que considere competente y notificarlo al solicitante, dentro del día hábil siguiente a su recepción.

Artículo 37.- Cuando sea derivada una solicitud donde el Sistema DIF Jalisco sea competente, se le dará el trámite correspondiente.

En caso de que el Sistema DIF Jalisco no sea competente, la UTIDIF deberá remitir, dentro del día hábil siguiente a su recepción, la solicitud de información al Instituto para que éste notifique al sujeto obligado competente.

Artículo 38.- La UTIDIF debe integrar un expediente por cada solicitud de acceso a la información pública recibida y asignarle un número único progresivo de identificación.

El expediente debe contener:

I. El original de la solicitud;

II. Las comunicaciones internas entre la UTIDIF y las Unidades Administrativas a las que se requirió información;

III. El original de la respuesta;

IV. Constancia de la notificación de la respuesta, en el caso que dicha respuesta sea remitida vía correo electrónico o física, en caso de que la notificación se realiza por el sistema INFOMEX, no será necesario integrarlo al expediente.

Artículo 39.- En la gestión interna de las solicitudes de información pública se procederá de la siguiente forma:

I. La UTIDIF previo turnar la solicitud a la Unidad Administrativa debe determinar la procedencia y competencia de esta, en su caso remitirla el mismo día de su admisión al área competente;

II. La Unidad Administrativa, en caso de inexistencia de la información solicitada, informará a la UTIDIF sobre ello antes de las quince horas del día siguiente en que recibió la solicitud;

III. Al interior de la Unidad Administrativa se requerirá la información solicitada y se entregará la respuesta a la UTIDIF, antes de las quince horas de los dos días hábiles siguientes a la recepción de la solicitud, con los datos siguientes:

a) Número de expediente de la solicitud de información;

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

b) Transcripción de lo solicitado;
c) Respuesta correspondiente a la solicitud;
d) Fundamentación y motivación;
e) Lugar y fecha; y
f) Nombre y firma del servidor público responsable de la información.

IV. En caso de que la Unidad Administrativa que posea la información solicitada, por la naturaleza y condiciones de la misma, requiera de un periodo mayor al establecido en el párrafo anterior, deberá comunicarlo por escrito a la UTIDIF, a fin de no incurrir en responsabilidad y poder estar en tiempo de contestar la solicitud.

V. En la generación y entrega de informes específicos, así como en las respuestas de inexistencia de información, se procederá de la misma forma que en los incisos precedentes, añadiendo además la justificación respectiva;

VI. En el procedimiento de clasificación inicial, se procederá de la misma forma que en la fracción III del presente artículo, incorporando además:

a) Los elementos de prueba de daño y consideración del interés público, con base en lo dispuesto en la Ley y los lineamientos del Instituto; y
b) Documento con la información sujeta a reserva parcial o total, con base en el procedimiento establecido en el artículo 28 del Reglamento.

VII. En los procedimientos de clasificación de información confidencial y de protección de información confidencial, se procederá de la misma forma que en la fracción III del presente artículo, incorporando además el documento con la información reservada como confidencial, así como la protegida, con base en el procedimiento establecido en el artículo 29 del Reglamento.

VIII. En el caso que la Unidad Administrativa no quiera proporcionar la información solicitada, se informa a Dirección General, así como al Instituto a fin de que se proceda con los procedimientos administrativos en contra del servidor público que correspondan.

Artículo 40.- Se deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, presumiendo la existencia de la información con base en los ordenamientos jurídicos aplicables a los mismos.

Artículo 41.- Para la declaratoria de inexistencia de información y en cumplimiento de las obligaciones en materia de transparencia y acceso a la información, se procederá conforme lo establece la Ley observando lo siguiente:

I. La Unidad Administrativa que manifieste la inexistencia de la información requerida no se refiere a alguna de sus facultades, competencias o funciones, notificará de

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

manera fundada y motivada a la UTIDIF, para resolver la solicitud en términos del artículo 86 Bis de la Ley;

II. En el supuesto que la información requerida sea inexistente y se refiera a alguna de sus facultades, competencias o funciones no ejercidas por la Unidad Administrativa, esta expondrá causas y circunstancias de tiempo y modo de su inexistencia, así como el funcionario o servidor público responsable de su generación y resguardo. La respuesta deberá incluir:

- **a)** Número de expediente de la solicitud de información;
- **b)** Transcripción de lo solicitado;
- **c)** Fundamentación y motivación de la inexistencia;
- **d)** Causas y circunstancias de la inexistencia, así como el servidor público o funcionario debió generarla y resguardarla;
- **e)** En el caso de pérdida o extravío de la información, indicar los procedimientos emprendidos para su recuperación o restitución;
- **f)** En el caso de robo o destrucción indebida de la información, indicar las procedimientos emprendidos para su recuperación y restitución, así como los procedimientos de responsabilidad administrativa, civil o penal iniciados;
- **g)** En el caso de fundar y motivar para acreditar la imposibilidad de su generación;
- **h)** Lugar y fecha de la respuesta; y
- **i)** Nombre y firma del funcionario o servidor público responsable de la información.

Artículo 42.- La respuesta de una solicitud de acceso a la información pública debe contener:

- **I.** Nombre del sujeto obligado correspondiente;
- **II.** Número de expediente de la solicitud;
- **III.** Datos de la solicitud;
- **IV.** Motivación y fundamentación sobre el sentido de la resolución;
- **V.** Puntos resolutivos sobre la procedencia de la solicitud, incluidas las condiciones para el acceso o entrega de la información, en su caso, y
- **VI.** Lugar, fecha, nombre y firma de quien resuelve.

Artículo 43.- La UTIDIF deberá observar en todas las respuestas sobre solicitudes de información que otorgue a los solicitantes lo siguiente:

- **I.** Emplear un lenguaje claro y sencillo;
- **II.** Traducir la respuesta en la lengua indígena, braille o cualquier formato accesible correspondiente cuando así lo manifieste el solicitante;

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

III. El nombre y cargo del titular de la Unidad Administrativa responsable de la respuesta a la solicitud de información.

Artículo 44.- La UTIDIF debe dar respuesta y notificar al solicitante, dentro de los ocho días hábiles siguientes a la admisión de la solicitud, respecto a la existencia de la información y la procedencia de su acceso, de acuerdo con esta ley y los lineamientos estatales de clasificación de información pública.

En la respuesta otorgada al solicite, la información se entrega en el estado que se encuentra y preferentemente en el formato solicitado. No existe obligación de procesar, calcular o presentar la información de forma distinta a como se encuentre.

Artículo 45.- La reproducción de documentos deberá cobrarse los costos de recuperación de los materiales por el monto del costo previsto en la Ley de Ingreso vigente en el estado, previo a la entrega de la información, expidiendo en forma gratuita las primeras veinte copias simples relativas a la información solicitada.

CAPÍTULO II
Del Acceso, Rectificación, Cancelación y Oposición de los Datos Personales

Artículo 46.- Se entenderá por datos personales, la información concerniente a una persona física identificada o identificable, entre otras, la relativa a su origen étnico o racial; la que se refiera a sus características físicas, morales o emocionales, a su vida afectiva o familiar; el domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales o cualquier otro dato análogo a los anteriores que afecten la intimidad de la persona.

Artículo 47.- En todo momento el titular o su representante podrán solicitar al responsable el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro.

Artículo 48.- A efecto de darle trámite a una solicitud de derecho ARCO, será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante.

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

En la acreditación del titular o su representante, el responsable deberá seguir las siguientes reglas:

I. El titular podrá acreditar su identidad a través de una Identificación oficial; Instrumentos electrónicos o mecanismos de autenticación permitidos por otras disposiciones legales o reglamentarias que permitan su identificación fehacientemente, habilitados por el responsable; o Aquellos mecanismos establecidos por el responsable de manera previa, siempre y cuando permitan de forma inequívoca la acreditación de la identidad del titular.

II. Cuando el titular ejerza sus derechos ARCO a través de su representante, éste deberá acreditar su identidad y personalidad presentando ante el responsable: Copia simple de la identificación oficial del titular; Identificación oficial del representante; e Instrumento público, o carta poder simple firmada ante dos testigos, o declaración en comparecencia personal del titular.

Artículo 49.- La solicitud debe hacerse en términos respetuosos y no podrán imponerse mayores requisitos que los siguientes:

I. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;
II. Nombre del solicitante titular de la información y del representante, en su caso;
III. Domicilio o cualquier otro medio para recibir notificaciones;
IV. Los documentos con los que acredite su identidad y, en su caso, la personalidad e identidad de su representante;
V. La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular;
VI. Descripción clara y precisa de los datos sobre los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso; y
VII. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

Artículo 50.- La UTIDF debe integrar un expediente por cada solicitud para el ejercicio de derechos ARCO y asignarle un número único progresivo de identificación.

El expediente deberá contener:

I. El original de la solicitud, con sus anexos, en su caso;
II. Las actuaciones de los trámites realizados en cada caso;
III. El original de la resolución; y
IV. Los demás documentos que señalen otras disposiciones aplicables.

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

Artículo 51.- El procedimiento de gestión de los Derechos ARCO será el siguiente:

I. La UTIDIF debe determinar la procedencia y competencia de esta y en su caso admitirla dentro de los tres día hábiles siguientes de su recepción;

II. Después de la admisión se le solicitara a la Unidad Administrativa, informe lo conducente respecto petición realizada por el solicitante.

III. En caso de inexistencia de la información solicitada, informará a la UTIDIF sobre ello antes de las quince horas del día otorgado para dar respuesta, con los datos siguientes:

- **a)** Número de expediente de la solicitud de información;
- **b)** Transcripción de lo solicitado;
- **c)** Respuesta correspondiente a la solicitud;
- **d)** Fundamentación y motivación;
- **e)** Lugar y fecha; y
- **f)** Nombre y firma del servidor público responsable de la información.

IV. Se convocara al Comité de Transparencia, a fin de resolver la solicitud de derecho ARCO, con la información proporcionada por la Unidad Administrativa.

V. En el caso que la Unidad Administrativa no quiera proporcionar la información solicitada, se informa a Dirección General, así como al Instituto a fin de que se proceda con los procedimientos administrativos en contra del servidor público que correspondan.

Cuando la solicitud de derecho ARCO sea de acceso y no haya alguna limitación legal, la UTIDIF podrá resolver dichas solicitudes sin necesidad de convocar al Comité

Artículo 52.- La resolución deberá contener:

I. Nombre del responsable correspondiente;
II. Número de expediente de la solicitud;
III. Datos de la solicitud;
IV. Motivación y fundamentación sobre el sentido de la resolución;
V. Puntos resolutivos sobre la procedencia de la solicitud; y
VI. Lugar, fecha, nombre y firma de quien resuelve.

Artículo 53.- Se deberá emitir la resolución dentro de los diez días siguientes a la admisión de la solicitud para el ejercicio de los derechos ARCO.

El plazo anterior podrá ampliarse por una sola vez hasta por cinco días, cuando así lo

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

justifiquen las circunstancias y siempre y cuando se le notifique al titular dentro del plazo de respuesta.

Artículo 54.- El ejercicio de los derechos ARCO deberá ser gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable.

En ningún caso, el pago de derechos deberá exceder el costo de reproducción, certificación o envío a que se refiere el párrafo anterior. Cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos deberán ser entregados sin costo a éste.

La información deberá ser entregada sin costo cuando implique la entrega de no más de veinte hojas simples. La UTIDIF podrá exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular.

TÍTULO QUINTO
De los Medios de Impugnación

CAPÍTULO ÚNICO

Artículo 55.- En caso de incumplimiento a las disposiciones de la Ley y el presente Reglamento, el solicitante o cualquier ciudadano podrán interponer ante el Instituto un medio de impugnación, contemplados en la Ley que son:

I. Recurso de Revisión;
II. Recurso de Transparencia;

Artículo 56.- Para la formulación de los informes de Ley de los recursos de revisión y de transparencia, la UTIDIF girará memorando a la Unidad Administrativa que conoció de la solicitud de información impugnada o que genere la información que debe estar publicada, para que en el término de veinticuatro horas manifiesten lo que a su derecho corresponda respecto al recurso.

La UTIDIF deberá remitir al Instituto un informe en contestación al recurso planteado, argumentando el actuar del Sujeto Obligado y adjuntando las constancias que acrediten su dicho.

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

Artículo 57.- En el supuesto que el Instituto en su resolución, ordene a los Sujetos Obligados alguna ejecución, se requerirá a las Unidades Administrativas, para que proporcionen a la UTIDIF la información necesaria para realizar el cumplimiento, lo cual deberán hacer apegándose al término concedido en la propia resolución, debiendo rendir la UTIDIF un informe de cumplimiento al Instituto.

En el caso que la Unidad Administrativa no quiera proporcionar la información solicitada, se rendirá informe en este sentido, además se informa a Dirección General, así como al Instituto a fin de que se proceda con los procedimientos administrativos en contra del servidor público que correspondan.

TÍTULO SEXTO
De las Sanciones

CAPÍTULO ÚNICO

Artículo 58.- Con independencia del cargo que ostente, el servidor público del Sistema DIF Jalisco que incumpla con lo dispuesto por la Ley y el presente Reglamento, se hará acreedor a las sanciones de tipo administrativo, civil o penal, que pudieran corresponder para el caso de la comisión de alguna conducta irregular o contraria a la Ley y normativa de la materia.

Artículo 58.- Serán causas de responsabilidad administrativa, civil o penal, según corresponda, a cargo de los servidores públicos que laboren en el Sistema DIF Jalisco, las contempladas en los artículos, del 118 al 124 de la Ley, por llegar a incurrir en alguno de los supuestos previstos en dicho apartado normativo.

TÍTULO SEPTIMO
De las Reformas al Reglamento

CAPÍTULO ÚNICO

Artículo 60.- Tendrán facultad para presentar iniciativas de reformas, adiciones o derogaciones al presente Reglamento, el Presidente y/o cualquier miembro del Comité de Transparencia.

Las iniciativas al presente Reglamento se ajustarán al siguiente procedimiento:

I. Será presentada por cualquiera de los miembros del Comité, en sesión, acompañada su propuesta de una exposición de motivos;

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

II. El Comité escuchará la propuesta y en su caso, la aprobará, modificará o rechazará;
III. La aprobación de la propuesta de reforma, adición o derogación, requerirá del voto de la mayoría de los miembros del Comité. En caso de ser aprobada será enviada a la Junta de Gobierno del Sistema DIF Jalisco, para el trámite correspondiente.

TRANSITORIOS

PRIMERO.- Se abrogan los Reglamentos Interno de la Unidad de Transparencia previamente aprobados por el Comité de Transparencia.
SEGUNDO.- El presente reglamento entrará en vigor al día siguiente de su aprobación.

TERCERO.- El Comité de Transparencia queda instalado conforme a lo sesionado el día 17 de diciembre del 2018.

Se elaboró el presente Reglamento Interno de la Unidad de Transparencia del Sistema para el Desarrollo Integral de la Familia de Jalisco, en la ciudad de Guadalajara, Jalisco con fecha de 27 de mayo de 2019, por el Comité de Transparencia.

Lic. Ana Lilia Mosqueda González
Presidenta del Comité de Transparencia

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

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

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

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 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 y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Museo Trompo Mágico

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar al edificio se cuenta con tres puertas metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina del Museo Trompo Mágico, se cuenta con otras puertas, con chapa de seguridad y en el interior de ella se tienen los archiveros donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el Museo Trompo Mágico son: • Marcela Gómez Ramírez, Museo Trompo Mágico;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo del 2019

Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en archivos digitales disco duro de las computadoras asignadas que cuentan con una clave de usuario, a lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar

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 los equipos de cómputo del Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar, para evitar que el personal no autorizado, tenga acceso a ellos; es que algunos equipos de cómputo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policia que resguarda las Instalaciones y una persona que controla ingresos a las mismas. Para ingresar al edificio se cuenta con una puerta metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas del Consejo, se cuenta con otras puertas, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el Consejo Estatal Para la Prevención y Atención de la Violencia Intrafamiliar: • Eunice Adriana Avilés Valencia, 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	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo del 2019

Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Unidad de Transparencia
Respecto del administrador de éste	**Nombre**	José de Jesús Segura de León
	Cargo	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 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.

Unidad de Transparencia 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, asi como en archivos digitales en memoria USB y en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Unidad de Transparencia del Sistema DIF Jalisco y sus Órganos Desconcentrados

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas son tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además para ingresar a las oficinas de la Unidad de Transparencia, se cuenta con puertas de madera, con chapa de seguridad y en el interior de ella se tienen archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Unidad de Transparencia son: • José de Jesús Segura de León, 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	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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**	Alejandra Salas Niño
	Cargo	Procuradura de Protección de Niñas, Niños y Adolescentes del Estado de Jalisco
	Adscripción	Procuraduría de Protección de Niñas, Niños y Adolescentes del Estado de Jalisco
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Jalisco, actual Titular de la Unidad de Transparencia; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Jalisco, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente, Autoridades del Sistema de Justicia, Fiscalía Estatal.
Inventario de los datos personales		**Datos Personales:** Nombre, edad, sexo, firma, características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, estado civil, Clave Única de Registro de Población (CURP). **Datos Personales Sensibles:** Adscripción o pertenencia étnica, condición de habla de lengua indígena, estado de salud física y mental, historial médico, información genética, datos biométricos, creencias religiosas, filosóficas y morales, preferencia sexual, condición o situación de derechos vulnerados y procesos de juridicos.
		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 Procuraduria de Protección de Niñas, Niños y Adolescentes.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, así como en archivos digitales disco duro de las computadoras asignadas con que se cuentan, teniendo una clave de usuario, a lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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 Procuraduria de Protección de Niñas, Niños, para evitar que personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa, pero carecen de llave; hay un control de acceso a las intalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con un oficial de policia que resguarda las Instalaciones y una persona que controla ingresos a las mismas. Para ingresar al edificio se cuenta con una puerta metalica con cristal y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a las oficinas de la Procuraduria de Protección de Niñas, Niños y Adolescentes, se cuenta con otras puertas, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta la Procuraduría de Protección de Niñas, Niños y Adolescentes: • Alejandra Salas Niño, Procuradora de Protección de Niñas, Niños y Adolescentes; • Norma de Jesús Villafaña Preciado, Directora de Prevención; • Rosa del Carmen Ochoa Cota, Directora de Atención y Protección; • Luis Antonio Gómez Hurtado, Director de Representación y Restitución; • María Raquel Arias Covarrubias; Directora de Tutela de Derechos; • Eunice Adriana Avilés Valencia, directora del CEPAVI;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Procuraduría de Protección a Niñas, Niños y Adolescentes

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Fecha de actualización del documento de seguridad	27 de mayo 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 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.

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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas se cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otra puerta de madera, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en esta Dirección son: • Luis Alberto Castro Rosales, Director Jurídico; • Diego Armando Calixto Guzmán, Jefe de Departamento de Control de Siniestros y Bienes Inmuebles; • Jorge Alberto Reséndiz Flores, Jefe de Unidad Departamental de Asuntos Laborales; • Francisco Alonso Moreno Muñoz, Jefe de Departamento de Acuerdos y Asuntos Jurídicos;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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**	Iván Valdez Rojas
	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 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 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 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 fisicamente 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros, con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha
Los expedientes se encuentran en archiveros 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 alfanuméricas de alta seguridad.
Gestión de vulneraciones

Órgano Interno de Control

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Contraloria, se cuenta con otra puertas metalicas y con cristal con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en las oficinas del Órgano Interno de Control son: • Iván Valdez Rojas, Titular del Órgano Interno de Control; • Alondra Dolores Vidrio Mendoza, Investigación; • Juana Elizabeth Guzmán Elías, Responsabilidades Administrativas;
Procedimientos de respaldo y recuperación de datos personales	Se cuenta en expediente físico.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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**	María del Rosario Salinas Villalobos
	Cargo	Directora de Recursos Humanos
	Adscripción	Dirección de Recursos Humanos
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Jalisco; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Jalisco, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**Datos Personales.-** Nombre, edad, sexo, firma, Características físicas, morales o emocionales, vida afectiva familiar, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, Clave Única de Registro de Población, Registro Federal de Contribuyentes, datos 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 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Dirección de Recursos Humanos

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas son tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina dela Dirección, se cuenta con puertas de madera y metal, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Recursos Humanos son: • María del Rosario Salinas Villalobos, Directora de Recursos Humanos; • Aurora Carolina González Hidalgo, Nóminas; • Yuriria Jazmín Tonanzing Ríos 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	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo del 2019

Dirección de Recursos Financieros

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Recursos Financieros
Respecto del administrador de éste	**Nombre**	Ana Elena González Jaime
	Cargo	Directora de Recursos Financieros
	Adscripción	Dirección de Recursos Financieros
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Jalisco; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Jalisco, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**Datos Personales.-** Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, Clave Única de Registro de Población, Registro Federal de Contribuyentes.
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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Dirección de Recursos Financieros

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otras puertas de metalicas con cristal, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Recursos Financieros son: • Ana Elena González Jaime, Directora de Recursos Financieros; • Jorge Ulises Segura Domínguez, Presupuestos; • Luz Angélica López Ortiz, Contabilidad; • Gildardo Mendoza Juárez. Tesorería;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

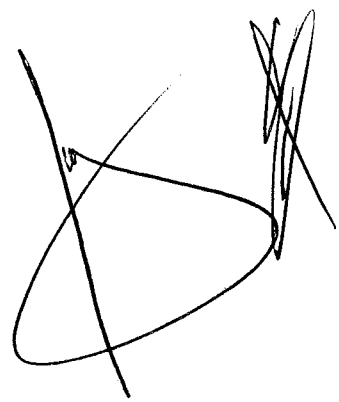
Mecanismos de monitoreo y revisión de las medidas de seguridad			Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.	
Programa General de capacitación				
Fecha			**Tipo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

Fecha de actualización del documento de seguridad	27 de mayo 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**	Iván Alejandro Bravo Reza
	Cargo	Director de Recursos Materiales
	Adscripción	Dirección de Recursos Materiales
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Jalisco; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Jalisco, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **Suprimir o devolver los datos personales** objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**Datos Personales.-** Nombre, edad, sexo, firma, domicilio particular, número de teléfono particular, correo electrónico particular, patrimonio, Clave Única de Registro de Población, Registro Federal de Contribuyentes.
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 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Dirección de Recursos Materiales

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otras puertas de metalicas con cristal, con chapa de seguridad y en el interior de ella se tienen los archiveros donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Recursos Materiales son: • Iván Alejandro Bravo Reza, Director de Recursos Materiales; • Alberto Clemente Preciado García, Activos Fijos; • Esther Fausto Brito, Almacén; • Roberto Alejandro Valladares Zamudio, Compras;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo del 2019

Dirección de Planeación Institucional

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales de la Dirección de Planeación 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 seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia, (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en los equipos de cómputo de la Dirección, para evitar que el personal no autorizado, tenga acceso a ellos; es que algunos equipos de cómputo cuenta con contraseñas alfanuméricas, aunque carecen de alta seguridad.
Gestión de vulneraciones

Dirección de Planeación Institucional

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policía que resguarda las Instalaciones y controla ingresos a las mismas.Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otras puertas de madera, con chapa de seguridad.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Planeación Institucional son: • Ernesto Jesús Ivon Pliego, Director de Planeación Institucional; • Héctor Juárez Ayard; Jefe de Departamento de Planeación y Desarrollo de Proyectos; • Karen Lizette Abreu Rodríguez, Jefa de Departamento de Evaluación y Seguimiento; • Alejandra Romo Arias, Jefa de Departamento de Profesionalización y Desarrollo Institucional;
Procedimientos de respaldo y recuperación de datos personales	Los archivos se encuentra en formatos digitales en cuentas asociadas al correo institucional.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otra puerta metalica, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Servicios Generales son: • 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	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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, asi como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran en archivos digitales en el Servidor del Organismo, a todo lo cual solo tiene acceso el personal responsable.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Dirección de Tecnologías y Sistemas de Información

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otras puertas de metalicas con cristal, con chapa de seguridad.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Tecnologías y Sistemas de Información son: • 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 Técnico;
Procedimientos de respaldo y recuperación de datos personales	Se tiene resguardada la información en el Servidor del Organismo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha

Dirección de Trabajo Social

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 policia custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanumericas de alta seguridad.
Gestión de vulneraciones
Por el momento no aplica este rubro, en virtud de que recientemente se implementó la bitacora de vulneraciones a la seguridad de los datos personales, sin que se haya registrado al momento incidente alguno.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otras puertas de metalicas con cristal, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Trabajo Social 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	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Dirección de Atención a las Personas Adultas Mayores

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otras puertas de metalicas con cristal, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección para el Desarrollo Integral del Adulto Mayor son: • María Asensión Álvarez Solís, Directora para el Desarrollo Integral del Adulto Mayor; • Yarib Michael Limón Villa, 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	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo del 2019

Dirección de Atención a la Infancia

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

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

Dirección de Atención a la Infancia

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policía que resguarda las instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otras puertas de metalicas con cristal, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Atención a la Infancia son: • José Martín Díaz de León Díaz de León, Director de Atención a la Infancia; • Angelina Tereshkova Juarez Ayard, Jefatura del Departamento de Estrategias de Atención a Infantes; • Tania Yahaira Ramirez 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	Al momento no se cuenta con un plan de contingencia.
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

Mecanismos de monitoreo y revisión de las medidas de seguridad	Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento.

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

Fecha de actualización del documento de seguridad	27 de mayo 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**	María Itzel Parada Lupercio
	Cargo	Directora 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 mandato expreso de la autoridad competente.
Inventario de los datos personales		**Datos Personales.-** Nombre, edad, sexo, fecha de nacimiento, nombre de los tutores, vida afectiva familiar, vida escolar, domicilio particular, número de teléfono particular, correo electrónico particular. **Datos Personales Sensibles.-** Diagnóstico médico, Estado de salud física y mental, historial médico, estudios neurológicos, evaluación de desarrollo de habilidades, reporte de avances terapéuticos.
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 Personas con Discapacidad

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 signada, a la cual tiene acceso el responsable de la Dirección y el personal a su cargo.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros, con llave, asi como en archivos digitales en el disco duro de la computadora asignada.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Gestión de vulneraciones

Dirección de Atención a Personas con Discapacidad

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con guardia de seguridad privada que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con una puerta metalica y cristal con chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otras puertas con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de Atención a Personas con Discapacidad son: • María Itzel Parada Lupercio, Dirección de Atención a Personas con Discapacidad; • Liliana Arcelia Gutierrez Gómez, Jefa del Departamento de Estrategias de Atención a Personas con Discapacidad; • Jehu Jonathan Preciado Pérez, Jefe del Departamento de Gestión de Centros de Atención para 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	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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 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.
		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 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 la computadora asignada, a la cual solo tiene acceso el personal responsable de la Dirección, cada trabajadora social operativa, y administrativa cuentan con los registros propios, para control y seguimiento.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.

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 u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otras puertas de metalicas con cristal, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de 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.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

Plan de trabajo

Dirección de Atención a Personas en Situación de Emergencia

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

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

Fecha de actualización del documento de seguridad	27 de mayo del 2019

Dirección de Comedores y Centros de Distribución de Alimentos

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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 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 disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable de la Dirección.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Dirección de Comedores y Centros de Distribución de Alimentos

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
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 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; • Marcela Guadalupe Aceves Sánchez, Subdirectora General de Seguridad Alimentaria.
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se tiene resguardada una copia escaneada en formato pdf de la información que el mismo contiene.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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 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 tiene acceso el responsable del Departamento y el personal a su cargo.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Dirección de Vinculación Municipal

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otras puertas de metalicas con cristal, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de 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 Ramirez 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	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo del 2019

Dirección de Control de la Gestión Institucional

FICHA DE PROTECCIÓN DE DATOS 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 Personales.-** 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 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 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Dirección de Control de la Gestión Institucional

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policia que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Dirección, se cuenta con otras puertas de metalicas con cristal, con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en la Dirección de 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	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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**	Luz Elena Perez Guzmán
	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 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta metálica con cristal y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, ademas con un filtro para el ingreso, ademas se cuenta con un guardia de seguridad privada que resgurda las instalaciones, para ingresar a las oficinas de los Centros de Atención, se cuenta con puertas con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el C.A.D.I. 02 son: • Luz Elena Perez Guzmán, Jefa del Departamento de C.A.D.I. 02;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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**	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, 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

Análisis de brecha

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

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta metálica con cristal y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, ademas con un filtro para el ingreso, ademas se cuenta con un guardia de seguridad privada que resgurda las instalaciones, para ingresar a las oficinas de los Centros de Atención, se cuenta con puertas con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el C.A.D.I. 06 son: • José Martín Díaz de León Díaz de León, Director de Atención a la Infancia; • Tania Yahaira Ramirez De La Rocha, Jefa del Departamento de Gestión en Centros de Atención Infantil;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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:** 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta metálica con cristal y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, ademas con un filtro para el ingreso, ademas se cuenta con un guardia de seguridad privada que resgurda las instalaciones, para ingresar a las oficinas de los Centros de Atención, se cuenta con puertas con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el C.A.D.I. 07 son: • Ruth Cisneros Martin, Jefa del Departamento de C.A.D.I. 07;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta metálica con cristal y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, ademas con un filtro para el ingreso, ademas se cuenta con un guardia de seguridad privada que resgurda las instalaciones, para ingresar a las oficinas de los Centros de Atención, se cuenta con puertas con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el C.A.D.I. 08 son: • Susana Fonseca Madrigal, Jefa del Departamento de C.A.D.I. 08;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo 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, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros con llave, asi como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitacora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitacora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

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

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

Centros de Atención de Desarrollo Infantil

FICHA DE PROTECCIÓN DE DATOS PERSONALES

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

Medidas de seguridad físicas aplicadas a las instalaciones	Para ingresar a los Centros de Atención se cuenta con una puerta metálica con cristal y chapa de seguridad, la cual es cerrada al término de actividades, restringiendo el ingreso. Además, ademas con un filtro para el ingreso, ademas se cuenta con un policia que resgurda las instalaciones, para ingresar a las oficinas de los Centros de Atención, se cuenta con puertas con chapa de seguridad y en el interior de ella se tienen los archiveros con chapa, en donde se resguardan los expedientes.
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en el C.A.D.I. 10 son: • Karen Alicia Mata Ornelas, Jefa del Departamento de C.A.D.I. 10;
Procedimientos de respaldo y recuperación de datos personales	Además del expediente físico, se cuenta con archivos digitales con los dátos básicos de cada expediente, en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de cómputo.
Plan de contingencia	Al momento no se cuenta con un plan de contingencia
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

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

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

Fecha de actualización del documento de seguridad	27 de mayo del 2019

DIF JALISCO

BITACORA DE ACCESO Y OPERACIÓN COTIDIANA A LOS DATOS PERSONALES

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

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

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

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

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.

Fecha de Actualización: *27 de Mayo de 2019.*

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

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 jurisdiccionales, con la finalidad de dar atención a los requerimientos judiciales o cualquier otro procedimiento seguido como un juicio; cualquier autoridad federal, estatal o municipal en ejercicio de sus funciones, que funde y motive la solicitud; el Instituto de Transparencia, Información Pública y Protección de Datos Personales (ITEI), las diferentes áreas de este sujeto obligado para poder dar seguimiento integral a la atención de los servicios que se prestan.*

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

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

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 Artículo 8, Fracciones VIII y IX.

Fecha de Actualización: *27 de Mayo de 2019.*

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

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; 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 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*

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

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 la integración de expedientes derivados de la atención o servicios que requiera usted como usuario del Sistema, 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 jurisdiccionales con la finalidad de dar atención a los requerimientos judiciales o cualquier otro procedimiento seguido como un juicio; cualquier autoridad federal, estatal o municipal en ejercicio de sus funciones, que funde y motive la solicitud; el Instituto de Transparencia, Información Pública y Protección de Datos Personales (ITEI); las diferentes áreas de este sujeto obligado para poder dar seguimiento integral a la atención de los servicios que presta se prestan.*

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 75 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,

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

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.

Fecha de Actualización: *27 de Mayo de 2019.*

Tel: 3030 3800
01 800 3000 343
Av. Alcalde # 1220,
Colonia Miraflores, C.P. 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 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 **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.

Fecha de Actualización: *27 de Mayo de 2019.*

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

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 jurisdiccionales con la finalidad de dar atención a los requerimientos judiciales o cualquier otro procedimiento seguido como un juicio; cualquier autoridad federal, estatal o municipal en ejercicio de sus funciones, que funde y motive la solicitud; el Instituto de Transparencia, Información Pública y Protección de Datos Personales (ITEI); las diferentes áreas de este sujeto obligado para poder dar seguimiento integral a la atención de los servicios que se prestan.*

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 343
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 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.

Fecha de Actualización: *27 de Mayo de 2019.*

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

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 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 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,*

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

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 **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 del Sistema, 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 jurisdiccionales con la finalidad de dar atención a los requerimientos judiciales o cualquier otro procedimiento seguido como un juicio; cualquier autoridad federal, estatal o municipal en ejercicio de sus funciones, que funde y motive la solicitud; el Instituto de Transparencia, Información Pública y Protección de Datos Personales (ITEI; las diferentes áreas de este sujeto obligado para poder dar seguimiento integral a la atención de los servicios que se prestan.*

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 75 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,*

Tel: 3030 3800
01 800 3000 343
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).

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.

Fecha de Actualización: *27 de Mayo de 2019.*

Tel: 3030 3800
01 800 3000 343
Av. Alcalde # 1220,
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.

Fecha de Actualización: *27 de Mayo de 2019.*

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

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 jurisdiccionales con la finalidad de dar atención a los requerimientos judiciales o cualquier otro procedimiento seguido como un juicio; cualquier autoridad federal, estatal o municipal en ejercicio de sus funciones, que funde y motive la solicitud; el Instituto de Transparencia, Información Pública y Protección de Datos Personales (ITEI); las diferentes áreas de este sujeto obligado para poder dar seguimiento integral a la atención de los servicios que se prestan.*

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

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

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.

Fecha de Actualización: *24 de Mayo de 2019.*

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

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; 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 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, edad, sexo, firma, domicilio particular, número de teléfono particular, correo electrónico particular, imagen, fotografía y video.*

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

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

atención o servicios que requiera usted como usuario, 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 jurisdiccionales con la finalidad de dar atención a los requerimientos judiciales o cualquier otro procedimiento seguido como un juicio; cualquier autoridad federal, estatal o municipal en ejercicio de sus funciones, que funde y motive la solicitud; el Instituto de Transparencia, Información Pública y Protección de Datos Personales (ITEI); las diferentes áreas de este sujeto obligado para poder dar seguimiento integral a la atención de los servicios que se prestan.*

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 75 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

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

Artículo 8, Fracciones VIII y IX.

Fecha de Actualización: *24 de Mayo de 2019.*