SEGUNDA SESIÓN ORDINARIA DEL COMITÉ DE TRANSPARENCIA DEL ORGANISMO PÚBLICO DESCENTRALIZADO DE LA ADMINISTRACION PUBLICA MUNICIPAL DENOMINADO SISTEMA PARA EL DESARROLLO INTEGRAL DE LA FAMILIA DEL MUNICIPIO DE GUADALAJARA, JALISCO.

En el Municipio de Guadalajara Jalisco y siendo las 14:30 catorce horas con treinta minutos del día 25 veinticinco del mes de septiembre del año 2024 dos mil veinticuatro, en las instalaciones del Organismo Público Descentralizado de la Administración Pública Municipal denominado Sistema para el Desarrollo Integral de la Familia del Municipio de Guadalajara, Jalisco; ubicado en la Avenida Eulogio Parra No. 2539 de la Colonia Lomas de Guevara, del Municipio de Guadalajara; se reunieron las siguientes personas: el **Lic. Miguel Escalante Vázquez** en su carácter de Titular de la Unidad de Transparencia y Secretario del Comité, la **Lic. en C.P. Berenice Cárabez Hernández** Contralora de este sujeto obligado e integrante del Comité, **Lic. José Antonio Castañeda Castellanos**, en su carácter de Presidente del Comité de Transparencia y Director Jurídico, ello con el objeto de dar inicio y desahogar la presente sesión ordinaria de conformidad con lo establecido en los artículos 29 y 30 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios. Por lo que en uso de la voz **el Lic. José Antonio Castañeda Castellanos,** Presidente del Comité de Transparencia de este sujeto obligado, quien preside la misma de conformidad con la fracción I del artículo 28 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios, dio lectura a la siguiente propuesta de:

ORDEN DEL DÍA

1.- Lista de asistencia, declaratoria de quórum legal, y apertura de la sesión.
2.- Lectura y aprobación del Orden del día.
3.- Presentación, discusión y en su caso aprobación de los documentos de Seguridad elaborados por las distintas áreas que conforman este Organismo.
4.- Asuntos Generales.
5.- Clausura de la Sesión.

DESARROLLO DEL ORDEN DEL DÍA

1.- Lista de Asistencia, declaratoria del quórum Legal y apertura de la sesión.- Voz del **Lic. José Antonio Castañeda Castellanos,** Presidente del Comité de Transparencia: le solicito al **Lic. Miguel Escalante Vázquez,** Secretario de este comité, nos haga favor de pasar la lista de asistencia a los presentes**:** Voz del **Lic. Miguel Escalante Vázquez:** Claro que sí Presidente: **¿Lic. José Antonio Castañeda Castellanos?,** ¡presente!, **¿Lic. Berenice Cárabez Hernández?,** ¡presente!, **¿Lic. Miguel Escalante Vázquez?,** ¡presente!. Voz del **Lic. José Antonio Castañeda Castellanos, Presidente del Comité de Transparencia del OPD denominado Sistema para el Desarrollo Integral de la Familia del Municipio de Guadalajara Jalisco.** Vista la verificación de la lista de asistencia y en razón de que nos encontramos todos los miembros del Comité de Transparencia, hago la correspondiente declaratoria del quórum legal, para la celebración de la presente sesión, por lo que todos los acuerdos tomados en esta sesión surtirán sus efectos legales correspondientes, de conformidad con el punto 2 del artículo 29 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios.

2.- Lectura y aprobación del Orden del día. Voz Lic. José Antonio Castañeda Castellanos, Presidente del Comité.- Le solicito al Lic. Miguel Escalante Vázquez, dé lectura al presente punto. **Voz Lic. Miguel Escalante Vázquez** en su carácter de Titular de la Unidad de Transparencia y Secretario del Comité: 1.- Lista de asistencia, declaratoria de quórum legal, y apertura de la sesión. 2.- Lectura y aprobación del Orden del día. 3.- Presentación, discusión y en su caso aprobación de los documentos de Seguridad elaborados por las distintas áreas que conforman este Organismo. 5.- Asuntos Generales. 6.- Clausura de la Sesión. **Voz Lic. José Antonio Castañeda**

Castellanos, Presidente del Comité: Previo a someter a votación el presente asunto, les pregunto si existe algún otro punto que tratar para ser votado e incluido en la sesión, a lo cual, se manifestó por el resto de los integrantes del Comité de Transparencia, que no había ningún otro asunto que tratar. **Voz Lic. José Antonio Castañeda Castellanos,** queda entonces aprobado por unanimidad de los presentes el orden del día propuesto, procediéndose al desahogo del mismo.

3.- Presentación, discusión y en su caso aprobación de los documentos de Seguridad elaborados por las distintas áreas que conforman este Organismo. Voz Lic. José Antonio Castañeda Castellanos.- Cedo el uso de la voz al Lic. Miguel Escalante Vázquez, secretario de este comité, para que dé cuenta del presente punto.

Voz Lic. Miguel Escalante Vázquez.- Comentarles que el artículo 35 de la la Ley de Protección de Datos Personales en posesión de sujetos obligados del Estado de Jalisco y sus Municipios establece la obligatoriedad de los entes de Gobierno, la elaboración de los documentos que contengan las medidas de seguridad administrativas, físicas y técnicas aplicables a sus sistemas de datos personales con el fin de asegurar la integridad, confidencialidad y disponibilidad de dichos datos que resguardan las Coordinaciones, Direcciones de Área, Jefaturas de Departamento y demás áreas que conforman este sujeto obligado, por lo que doy cuenta que se recibieron las propuestas de los documentos de seguridad de las unidades administrativas que recaban y resguardan datos personales, mismos que cumplen a cabalidad los requisitos establecidos en el artículo 36 de la citada Ley de Protección de Datos Personales, en posesión de sujetos obligados del Estado de Jalisco y sus Municipios.

En cumplimiento de lo establecido en las fracciones I y V del artículo 87 de la Ley de Protección de Datos Personales en posesión de sujetos obligados del Estado de Jalisco y sus Municipios, se propone a los miembros de este Órgano Garante lo siguiente:

a) La validación y aprobación de los documentos de seguridad de este Organismo.
b) Una vez aprobados, se autorice la publicación de dichos documentos de seguridad, con excepción de los siguientes elementos: estructura y descripción de los sistemas de tratamiento y/o bases de datos personales, almacenamiento, los análisis de riesgos, los análisis de brechas, el plan de contingencia, el plan de trabajo, el monitoreo y revisión de las medidas de seguridad. Esta decisión se fundamenta en la consideración de que estos aspectos son de naturaleza estratégica para las unidades administrativas y podrían potencialmente poner en riesgo la seguridad y protección de los datos personales recopilados y resguardados por las mismas.

Voz Lic. José Antonio Castañeda Castellanos Presidente del Comité: Si no hay más intervenciones, le solicito al Lic. Miguel Escalante Vázquez, Secretario de este Comité, haga favor de someter a votación el presente punto para su aprobación. **Voz C. Miguel Escalante Vázquez, Secretario del Comité:** ¿quienes estén a favor, de aprobar el los documentos de seguridad, así como la publicación de los mismos en los términos planteados, lo externen levantando la mano? **Voz Lic. José Antonio Castañeda Castellanos** Presidente del Comité: Aprobado por unanimidad.

5.- Asuntos Generales.- Voz Lic. José Antonio Castañeda Castellanos Presidente del Comité: ¿Existe algún tema adicional a tratar en esta sesión? Al no existir tema alguno por tratar en la presente sesión, pasamos a la clausura de la Sesión.

6.- Clausura de la Sesión. - Voz Lic. José Antonio Castañeda Castellanos Presidente del Comité: No habiendo más asuntos a tratar, doy por clausurada la presente sesión, siendo las 15:33 quince horas con treinta y tres minutos del día de hoy miércoles 25 de septiembre del año 2024 dos mil veinticuatro; agradeciendo su asistencia ¡Gracias! Levantándose la presente acta en vía de constancia, firmando en ella quienes intervinieron.

Lic. José Antonio Castañeda Castellanos
Director Jurídico y Presidente del Comité de Transparencia del OPD denominado del Sistema DIF Guadalajara

Lic. Miguel Escalante Vázquez
Titular de la Unidad de Transparencia y Secretario del Comité de Transparencia del OPD denominado Sistema del Sistema DIF Guadalajara

Lic. en C.P. Berenice Cárabez Hernández
Contralora y Miembro del Comité de Transparencia del OPD denominado Sistema del Sistema DIF Guadalajara.

DIF
Guadalajara

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS PERSONALES.

ORGANISMO PUBLICO DESCENTRALIZADO DE LA ADMINISTRACIÓN PÚBLICA MUNICIPAL DENOMINADO SISTEMA PARA EL DESARROLLO INTEGRAL DE LA FAMILIA DE GUADALAJARA

ADMINISTRACIÓN 2021 – 2024

I.- Introducción:

El presente documento, contiene las disposiciones en materia de protección de datos personales de las unidades administrativas que forman parte de este Organismo Público Descentralizado.

En el Sistema Para el Desarrollo Integral de la Familia de Guadalajara, la información es un activo que debe protegerse, mediante procesos y sistemas diseñados, administrados y mantenidos por el Organismo. Por ello, la gestión de la seguridad de la información busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información que posee.

El día 26 de enero del año 2017, fue publicada en el Diario Oficial de la Federación, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en tanto que, seis meses después, es decir, el día 26 de julio del mismo año, también fue publicada en el periódico oficial "El Estado de Jalisco", la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios. En ambas legislaciones se establecen las bases, principios y procedimientos para garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de sujetos obligados de los tres órdenes de gobierno; se definen las bases mínimas y condiciones homogéneas que regirán el tratamiento de datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (Derechos ARCO) mediante procedimientos sencillos y expeditos; asimismo, se establece la protección de los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las Entidades Federativas y los municipios, con la finalidad de regular su debido tratamiento.

En virtud de lo anterior y de conformidad con lo establecido en los artículos 3 fracción XIV y 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en relación con los diversos 3 fracción XIV y 36 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, se elabora el presente documento de seguridad con la finalidad de dar cumplimiento a lo establecido en estos cuerpos normativos.

OBJETIVO

El presente documento tiene como objetivo establecer los procedimientos implementados en materia de seguridad y protección de datos personales, conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales, previstos en las legislaciones referidas en el párrafo que antecede.

GLOSARIO

I. Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

II. Aviso de privacidad: Documento físico, electrónico o en cualquier formato generado por el responsable, que es puesto a disposición del titular con el objeto de informarle los propósitos principales del tratamiento al que serán sometidos sus datos personales;

III. Bases de Datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

IV. Bloqueo: La identificación y conservación de los datos personales, una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual correspondiente. Durante dicho período los datos personales no podrán ser objeto de tratamiento y concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente o sistema de información que corresponda;

V. Comité de Transparencia: Comité de Transparencia de cada sujeto obligado en los términos de la Ley de Transparencia, en esta Ley y demás disposiciones aplicables;

VI. Consentimiento: Manifestación de la voluntad libre, específica e informada del titular que autoriza el tratamiento de sus datos personales;

VII. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

VIII. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

IX. Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

X. Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

XI. Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

XII. Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable;

XIII. Evaluación de impacto en la protección de datos personales: documento mediante el cual se valoran y determinan los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en esta Ley y demás disposiciones aplicables;

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

XV. Instituto Nacional: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XVI. Ley: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Jalisco y sus Municipios;

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

XVIII. Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

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

XX. Medidas de seguridad: conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales;

XXI. Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización, formación y capacitación del personal, en materia de protección de datos personales;

XXII. Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

XXIII. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento.

XXIV. Remisión: toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, con independencia de que se realice dentro o fuera del territorio mexicano;

XXV. Responsable: Los sujetos obligados señalados en el artículo 1, párrafo 5, de la presente Ley que determinarán los fines, medios y alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

XXVI. Supresión: la baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

XXVII. Titular: Persona física a quien pertenecen los datos personales;

XXVIII. Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado;

XXIX. Tratamiento: De manera enunciativa más no limitativa cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales; y

XXX. Unidad de Transparencia: instancia que funge como vínculo entre el responsable y el titular, siendo la misma a la que se hace referencia en el artículo 31 de la Ley de Transparencia y en la presente Ley.

MARCO JURÍDICO

Para efectos del presente documento, la normatividad aplicable es la siguiente:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Constitución Política del Estado de Jalisco.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios

II.- De los Sistemas de Tratamiento:

Se diseñaron los siguientes Sistemas de Tratamiento:

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Área de Comunicación Social
Administrador de Archivos y base de datos	**Nombre**	Stefany Esquivel Velázquez
	Cargo	Titular del Área de Comunicación Social
	Adscripción	Dirección General del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
Stefany Esquivel Velázquez. Titular del Área de Comunicación Social	Uso, cancelación.	Coteja la documentación de los expedientes para dar validez con su firma.
Harol Humberto Jiménez Quintero. Supervisor	Obtención, almacenamiento, uso, divulgación.	Recepción de solicitudes de apoyo para capturar imagen o voz de personas beneficiarias, mediante fotografías y videograbaciones, integración de expedientes, publicación siempre y cuando haya autorización expresa de su titular.
José Luis Rivas Salcido. Soporte.	Obtención, almacenamiento, uso, divulgación.	Recepción de solicitudes de apoyo para capturar imagen o voz de personas beneficiarias, mediante fotografías y videograbaciones, integración de expedientes, publicación siempre y cuando haya autorización expresa de su titular.
Mario Alberto Rodríguez Monroy. Analista A	Obtención, almacenamiento, uso, divulgación.	Recepción de documentación, integración de expedientes, protección de datos personales.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, edad, firma, fotografía y voz.	Directa/Presencial	El nivel de riesgo es bajo. Los datos personales son de categoría estándar, es decir, no sensibles.
Datos identificativos de niñas, niños y adolescentes: nombre, edad, fotografía y voz.	Indirecta/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen por conducto de su representante legal o tutor.	El nivel de riesgo es medio. Los datos personales son de categoría especial, y aunque no sensibles, corresponden a niñas, niños y adolescentes.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Previo a la grabación videográfica o fotográfica de algún evento, se convoca a los titulares de los datos personales o representantes o tutores de los menores de edad, quienes acuden de forma presencial a otorgar autorización expresa y por escrito, para la utilización de su imagen, su voz y sus datos personales o los de sus hijos o representados menores de edad.	Recabar información para formar un expediente con base a una solicitud y dar un seguimiento a la misma hasta su conclusión, de conformidad con los artículos 38 y 41 fracciones I a la V del Reglamento Interno de este Organismo.

Almacenamiento	2.eliminado
Uso	El uso de las fotografías y videos, con la imagen, voz y datos personales de sus titulares, de sus menores hijos o representados, se usa exclusivamente en promocionales y demás materiales de comunicación Institucional, para la difusión y promoción de actividades que realiza el DIF Guadalajara.
Divulgación	**Remisiones:** Se remiten los expedientes con la Coordinación de Inclusión, Coordinación de Programas y Coordinación de Operación y sus áreas que las conforman. **Transferencias:** Se realizan con el Gobierno Municipal de Guadalajara quien tiene el carácter de "responsable" y siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales (por cualquier causa), se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: Transferencias mediante el traslado de soportes físicos: a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. Transferencias mediante el traslado físico de soportes electrónicos: Los datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB, se trasladan con contraseñas y se siguen todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. Transferencias mediante el traslado sobre redes electrónicas: a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Características del Lugar de Resguardo: Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.

Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Titular del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

memorias USB o tarjetas SD en el tratamiento de datos personales.

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Contraloría Interna
Administrador de Archivos y base de datos	**Nombre**	Berenice Carabez Hernández
	Cargo	Contralora Interna
	Adscripción	Contraloría Interna del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
Berenice Carabez Hernández. Contralora Interna	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en un expediente y posterior a ello, brindar autorización y validez con su firma.
María de Jesús Valdez Romo. Jefatura del Área de Auditoria	Obtiene, almacena, usa, remite y suprime.	Inicio de auditorías o visitas de inspección, integración y análisis de expediente, proyecta determinaciones, observaciones o recomendaciones. Dar vista al área de investigación cuando así proceda.
Edgar Israel Martínez Rubi. Jefatura del Área de Investigación	Obtiene, almacena, usa, remite y suprime.	Recepción de declaraciones de situación patrimonial, de intereses y constancia de presentación de declaración fiscal; recepción e investigación de quejas o denuncias, integración de expediente, análisis y elaboración de informe de presunta responsabilidad administrativa y turnarlo al área de substanciación y resolución cuando proceda.
Gustavo Gilberto Puga Gómez. Jefatura del Área de Substanciación y Resolución	Obtiene, almacena, usa, remite y suprime.	Recepción de informe de presunta responsabilidad administrativa, integración y análisis de expediente y proyectar resolución.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, domicilio, estado civil, Registro Federal de Contribuyentes, (RFC), teléfono particular, teléfono celular, firma, clave única de registro de población (CURP), clave de elector, lugar y fecha de nacimiento, nacionalidad, edad, estado civil, fotografía, y huella digital.	Directa (Presencial) o indirecta (electrónica) (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo. Los datos personales son de categoría estándar a excepción de la huella dactilar que es un dato personal sensible
Datos sobre la salud: Estado de salud físico o mental de la persona.	Directa (Presencial) e indirecta (electrónica).	El nivel de riesgo es medio. Los datos personales son sensibles
Datos laborales: Nombramiento, referencias laborales.	Directa (Presencial) e indirecta (electrónica).	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos patrimoniales: Los correspondientes a bienes muebles e inmuebles, información fiscal, ingresos y egresos, beneficiarios, dependientes económicos.	Directa (Presencial) e indirecta (electrónica).	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos académicos: Trayectoria educativa, título, cédula profesional.	Directa (Presencial) e indirecta (electrónica).	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos sobre situación jurídica o legal: La información relativa a una persona que se encuentre o haya sido sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa.	Directa (Presencial) e indirecta (electrónica).	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.

Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Los titulares de los datos personales o representantes o tutores de los menores de edad, proporcionan datos personales de forma presencial o electrónica, para la integración de expedientes en virtud de quejas o denuncias por inconformidades en materia de compras gubernamentales, realización de auditorías, denuncias por presuntas responsabilidades cometidas por empleados del Organismo, así como la substanciación de procedimientos de responsabilidad administrativa. De igual forma se obtienen por motivo de la declaración de situación patrimonial y de intereses de los empleados.	Recabar información para formar un expediente con base a la interposición de queja o denuncia y dar un seguimiento a la misma hasta su conclusión. Asimismo, para llevar a cabo auditorias y para recibir declaraciones de situación patrimonial y de intereses de conformidad con los artículos 190 al 200 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Emitir la resolución o sentencia correspondiente, respecto a las quejas o denuncias presentadas. Acreditar que se realizó la declaración patrimonial y de intereses y; Emitir observaciones en el caso de auditorías.	
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. **Transferencias:** Se realizan hacia autoridades que tienen el carácter de "responsables", como la Contraloría Ciudadana del Municipio de Guadalajara, Sistema Estatal Anticorrupción, Fiscalía Especializada en Combate a la Corrupción y Tribunal de Justicia Administrativa, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf	
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.	
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.	

Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos: N**o realizan transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.
Análisis de riesgos	
3.eliminado	

concentración a una área segura y sin este tipo de problemas.

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo	
6.eliminado	
Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Dirección del Área Centros de Inclusión
Administrador de Archivos y base de datos	**Nombre**	María Zenyasse Flores Aceves
	Cargo	Directora del Área de Centros de Inclusión
	Adscripción	Coordinación de Inclusión del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
María Zenyasse Flores Aceves. Directora del Área	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo asistencial y en caso de proceder, brinde autorización y validez con su firma.
Ana Alejandra Quijada Briseño. Jefatura del Departamento de Centro de Autismo y Discapacidad Intelectual	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de atención integral para personas con Trastorno del Espectro Autista y Discapacidad Intelectual, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, clave única de registro de población (CURP), edad, fotografía, clave de elector, número de pasaporte.	Directa/Presencial (en caso de niñas, niños o adolescentes, o de personas con TAE o discapacidad intelectual, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es medio. Los datos personales son de categoría especial, por corresponder a niñas, niños y adolescentes y/o personas con TAE o discapacidad intelectual.
Datos sobre la salud: expediente clínico de cualquier atención médica, historial médico, referencias o descripción de sintomatologías, detección de enfermedades, discapacidades, intervenciones quirúrgicas, uso de aparatos ortopédicos, auditivos, estado físico o mental de la persona.	Directa/Presencial (en caso de niñas, niños o adolescentes, o de personas con TAE o discapacidad intelectual, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es medio. Los datos personales son de categoría especial, por corresponder a niñas, niños y adolescentes y/o personas con TAE o discapacidad intelectual.
Datos patrimoniales: Los correspondientes a ingresos y egresos.	Directa/Presencial	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	Los titulares de los datos personales o representantes o tutores de los menores de edad, sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo para realizar una evaluación y diagnóstico para corroborar o descartar la presencia del TAE, para recibir terapia de lenguaje, terapia para personas con Trastorno del Espectro Autista, terapia para personas con Discapacidad Intelectual, para admisión a cualquiera de los talleres prelaborales, de estimulación cognitiva, de atención psicológica familiar, de rehabilitación y psicomotricidad y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con los artículos 178 y 181 del Reglamento Interno de este Organismo.

Almacenamiento	2.eliminado
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de manera interinstitucional, es decir, hacia autoridades que tienen el carácter de "responsables", tales como el Sistema DIF Jalisco, o a los Sistemas DIF Municipales, que briden servicios de Rehabilitación, de atención a personas con TAE o con discapacidad intelectual, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** En esta Dirección, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.

Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Departamento de Desarrollo Integral de Personas Adultas Mayores (DIPAM)
Administrador de Archivos y base de datos	**Nombre**	Leticia Guadalupe Romero Lima
	Cargo	Jefatura del Departamento de Desarrollo Integral de Personas Adultas Mayores (DIPAM)
	Adscripción	Coordinación de Inclusión del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Leticia Guadalupe Romero Lima. Jefe del Departamento de Desarrollo Integral de Personas Adultas Mayores (DIPAM)	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo asistencial y en caso de proceder, brinde autorización y validez con su firma.
Livia Teresa Flores Livia Teresa Flores Garnelo. Supervisor Agustín Sevilla Gómez. Soporte	Obtención, almacenamiento, uso, divulgación.	Recepción de reportes/solicitudes de atención a adultos mayores en desamparo, marginación o maltrato, de expedición de credencial de adulto mayor, de asesoría de trabajo social y jurídica, de actas testimoniales para registro extemporáneo, trámite de testamento ológrafo, de consulta médica y expedición de certificado médico, de atención gerontológica, de admisión al comedor asistencial, a casas de día, a grupos de personas adultas mayores o a los talleres ocupacionales, recreativos, culturales, de manualidades y deportivos, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, edad, fotografía, CURP.	Directa/Presencial e Indirecta/electrónica/telefónica	El nivel de riesgo es bajo. Los datos personales son de categoría estándar, con excepción de los que pertenezcan a personas que reciben atención médica, o que se encuentran en abandono, cuyo nivel de riesgo es medio y de categoría especial.
Datos sobre la salud: Referencias o descripción de sintomatologías, detección de enfermedades, estado físico o mental de la persona. (estos datos solo se obtienen en caso de personas que solicitan atención médica).	Directa/Presencial e Indirecta/electrónica/telefónica	El nivel de riesgo es medio. Los datos personales son de categoría especial, por corresponder a personas que reciben atención médica.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	Los titulares de los datos personales sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable. En caso de reportes/solicitudes de atención a adultos mayores en desamparo, marginación o maltrato los datos personales también pueden ser obtenidos mediante llamada telefónica.	Recabar información para formar un expediente con base a la recepción de reportes/solicitudes de atención a adultos mayores en desamparo, marginación o maltrato, solicitudes de expedición de credencial de adulto mayor, de asesoría de trabajo social y jurídica, de actas testimoniales para registro extemporáneo, trámite de testamento ológrafo, de consulta médica y expedición de certificado médico, de atención gerontológica, de admisión al comedor asistencial, a casas de día, a grupos de personas adultas mayores o a los talleres ocupacionales, recreativos, culturales, de manualidades y deportivos y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con el artículo 185 del Reglamento Interno de este Organismo.

Almacenamiento	2.eliminado
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.
Divulgación	**Remisiones**: Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de la siguiente manera: En el caso de personas adultas mayores en abandono o desamparo: **1.-** A terceros con los cuales el Organismo celebre convenios de colaboración para la guarda y cuidado de estas personas, mismos que asumen el carácter de "encargados", por lo que solo realizan las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de los mismos y limitan su actuación a los términos fijados por este Organismo en su calidad de "responsable". Esta relación entre el responsable y el encargado, se formaliza mediante contrato, convenio o instrumento jurídico, en cuyo clausulado el encargado de obliga a: a).- Realizar el tratamiento de los datos personales conforme a las instrucciones que se le den; b).- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas; c).- Informar a este Organismo cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; d).- Guardar confidencialidad respecto de los datos personales tratados; e).- 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); f).- Abstenerse de transferir los datos personales salvo que el responsable así lo determine; la comunicación derive de una subcontratación y medie la autorización expresa de este Organismo; o por mandato expreso de la autoridad competente; **2.-** De manera interinstitucional, se realizan hacia autoridades que tienen el carácter de "responsables" tales como la Procuraduría Social del Estado para trámite de asesoría, al el Sistema DIF Jalisco y a los 125 Sistemas DIF Municipales del Estado de Jalisco, a fin de que brinden el apoyo asistencial correspondiente, a la Fiscalía Estatal para el inicio de carpeta de investigación, mediante la presentación de denuncia, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, o bien por corresponder a su competencia territorial. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Este Departamento, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.

El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) jefe(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Departamento de Centro de Atención Integral para Personas con Discapacidad (CAIPED)
Administrador de Archivos y base de datos	**Nombre**	Daniela Dolores Curiel Rodríguez
	Cargo	Jefatura del Departamento de Centro de Atención Integral para Personas con Discapacidad (CAIPED)
	Adscripción	Coordinación de Inclusión del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
Daniela Dolores Curiel Rodríguez. Jefa del Departamento de Centro de Atención Integral para Personas con Discapacidad (CAIPED)	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo asistencial y en caso de proceder, brinde autorización y validez con su firma.
Bibiana de los Ángeles Navarro Diaz. Coordinador de Proyecto Francisco Alejandro Espinoza Vargas. Soporte	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de atención especializada en medicina en rehabilitación, en rehabilitación acuática, en traumatología, en terapia psicológica, terapia física, en podología, en terapia de lenguaje, de acceso a auxiliares auditivos de bajo costo, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, domicilio, clave única de registro de población (CURP), edad, fotografía, clave de elector, número de pasaporte.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor).	El nivel de riesgo es medio. Los datos personales son de categoría especial, por corresponder a niñas, niños y adolescentes y/o a personas con algún problema de salud o discapacidad física.
Datos sobre la salud: expediente clínico de cualquier atención médica, historial médico, referencias o descripción de sintomatologías, discapacidades, uso de aparatos ortopédicos, auditivos.	Directa/Presencial (en caso de niñas, niños o adolescentes, o de personas con TAE o discapacidad intelectual, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es medio. Los datos personales son de categoría especial, por corresponder a niñas, niños y adolescentes y/o a personas con algún problema de salud o discapacidad física.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Los titulares de los datos personales o representantes o tutores de los menores de edad, sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo de atención especializada en medicina en rehabilitación, en rehabilitación acuática, en traumatología, en terapia psicológica, terapia física, en podología, en terapia de lenguaje, de acceso a auxiliares auditivos de bajo costo y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con los artículos 187 del Reglamento Interno de este Organismo.

Almacenamiento	2.eliminado
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de la siguiente manera: En el caso de personas que requieren auxiliares auditivos: 1.- A terceros con los cuales el Organismo celebre convenios de colaboración para proporcionar auxiliares administrativos a bajo costo o que tengan el carácter de proveedores, mismos que asumen el carácter de "encargados", por lo que solo realizan las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de los mismos y limitan su actuación a los términos fijados por este Organismo en su calidad de "responsable". Esta relación entre el responsable y el encargado, se formaliza mediante contrato, convenio o instrumento jurídico, en cuyo clausulado el encargado de obliga a: a).- Realizar el tratamiento de los datos personales conforme a las instrucciones que se le den; b).- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas; c).- Informar a este Organismo cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; d).- Guardar confidencialidad respecto de los datos personales tratados; e).- 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); f).- Abstenerse de transferir los datos personales salvo que el responsable así lo determine; la comunicación derive de una subcontratación y medie la autorización expresa de este Organismo; o por mandato expreso de la autoridad competente; 2.- De manera interinstitucional, se realizan hacia autoridades que tienen el carácter de "responsables" tales como el Sistema DIF Jalisco y a los 125 Sistemas DIF Municipales del Estado de Jalisco, a fin de que brinden el apoyo asistencial correspondiente, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, o bien por corresponder a su competencia territorial. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Este Departamento, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.

El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Jefe(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Departamento de Proyectos de Inclusión
Administrador de Archivos y base de datos	**Nombre**	León Gerardo Silva Contreras
	Cargo	Jefatura del Departamento de Proyectos de Inclusión
	Adscripción	Coordinación de Inclusión del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
León Gerardo Silva Contreras. Jefe del Departamento de Proyectos de Inclusión	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo asistencial y en caso de proceder, brinde autorización y validez con su firma.
Miriam Guadalupe García Castañeda. Soporte	Obtención, almacenamiento, uso, divulgación.	Recepción de solicitudes de expedición de gancho de estacionamiento, de admisión para capacitación en cursos de sensibilización, de Lengua de Señas Mexicana, de lectoescritura en braille, solicitudes de canalización a empresas y negocios incluyentes con vacantes de empleo para personas con discapacidad, así como de atención a personas declaradas incapaces que se encuentren en albergues, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, edad, fotografía, clave de elector, número de pasaporte.	Directa/Presencial	El nivel de riesgo es bajo. Los datos personales son de categoría estándar, con excepción de los que pertenezcan a personas declarados incapaces o con alguna discapacidad, cuyo nivel de riesgo es medio y de categoría especial.
Datos sobre la salud: expediente clínico de cualquier atención médica, historial médico, detección de enfermedades, discapacidades, intervenciones quirúrgicas, estado físico o mental de la persona. (estos datos solo se obtienen en caso de personas declarados incapaces o con alguna discapacidad).	Directa/Presencial (en caso de personas declarados incapaces, los datos personales se obtienen mediante la remisión de asuntos realizados por la Delegación Institucional de Protección de Niñas, Niños y Adolescentes, cuando estos cumplen la mayoría de edad).	El nivel de riesgo es medio. Los datos personales son de categoría especial, por corresponder a personas con algún tipo de discapacidad intelectual.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	Los titulares de los datos personales sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable. En caso de personas declarados incapaces, los datos personales se obtienen mediante la remisión de asuntos realizados por la Delegación Institucional de Protección de Niñas, Niños y Adolescentes, cuando estos cumplen la mayoría de edad).	Recabar información para formar un expediente con base a la solicitud de apoyo para expedición de gancho de estacionamiento, de admisión para capacitación en cursos de sensibilización, de Lengua de Señas Mexicana, de lectoescritura en braille, solicitudes de canalización a empresas y negocios incluyentes con vacantes de empleo para personas con discapacidad, así como de atención a personas declaradas incapaces que se encuentren en albergues y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con el artículo 183 del Reglamento Interno de este Organismo.

Almacenamiento	2.eliminado
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.
Divulgación	**Remisiones**: Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de la siguiente manera: En el caso de personas declaradas incapaces **1.-** A terceros con los cuales el Organismo celebre convenios de colaboración para la guarda y cuidado de estas personas, mismos que asumen el carácter de "encargados", por lo que solo realizan las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de los mismos y limitan su actuación a los términos fijados por este Organismo en su calidad de "responsable". Esta relación entre el responsable y el encargado, se formaliza mediante contrato, convenio o instrumento jurídico, en cuyo clausulado el encargado de obliga a: a).- Realizar el tratamiento de los datos personales conforme a las instrucciones que se le den; b).- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas; c).- Informar a este Organismo cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; d).- Guardar confidencialidad respecto de los datos personales tratados; e).- 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); f).- Abstenerse de transferir los datos personales salvo que el responsable así lo determine; la comunicación derive de una subcontratación y medie la autorización expresa de este Organismo; o por mandato expreso de la autoridad competente; **2.-** En el caso de personas con discapacidad que buscan empleo, se realizan canalización a terceros (empresas y negocios incluyentes con vacantes de empleo) con los cuales el Organismo tiene celebrado algún convenio de colaboración, sin embargo, en este supuesto estos terceros adquieren el carácter de responsables en el tratamiento de los datos personales, pues es para efectos de su contratación laboral. **3.-** De manera interinstitucional, se realizan hacia autoridades que tienen el carácter de "responsables" tales como el Gobierno de Guadalajara, el Sistema DIF Jalisco y a los 125 Sistemas DIF Municipales del Estado de Jalisco, a fin de que brinden el apoyo asistencial correspondiente, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, o bien por corresponder a su competencia territorial. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Este Departamento, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.

El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Jefe(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Departamento de Atención y Desarrollo Integral para Personas en Situación de Calle. (CADIPSIC)
Administrador de Archivos y base de datos	**Nombre**	Octavio Manuel Oláez Robles.
	Cargo	Jefatura del Departamento de Atención y Desarrollo Integral para Personas en Situación de Calle.
	Adscripción	Coordinación de Inclusión del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Octavio Manuel Oláez Robles. Jefe del Departamento de Atención y Desarrollo Integral para Personas en Situación de Calle. (CADIPSIC)	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo asistencial y en caso de proceder, brinde autorización y validez con su firma.
José Javier Zamorano Farías. Jefe de Turno Xóchitl Araceli Ambriz Rivera. Jefe de Turno de Atención Social. David Andrés Chávez Ramírez. Jefe de Turno de Salud Elizabeth Hernández Cervantes. Jefe de Turno de Brigada. Jesús Norberto Villaseñor Montes. Coordinador de Proyecto	Obtención, almacenamiento, uso, divulgación.	Recepción de solicitudes de refugio para dormir, de apoyo humanitario en calle con alimentos, cobijas, impermeables; de solicitud de derivación a albergue privado; solicitud de estancia temporal con atención de salud, alimentos, de educación y psicológica; solicitud de estancia nocturna con atención médica, de trabajo social, de atención psicológica, regularización académica y de apoyos asistenciales mediante entrega de kit de higiene, de calzado y cobija; integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, edad, fotografía, CURP.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo. Los datos personales son de categoría estándar, con excepción de los que pertenezcan a personas que reciben atención médica, cuyo nivel de riesgo es medio y de categoría especial.
Datos sobre la salud: Referencias o descripción de sintomatologías, detección de enfermedades, estado físico o mental de la persona. (estos datos solo se obtienen en caso de personas que solicitan atención médica).	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo. Los datos personales son de categoría estándar, con excepción de los que pertenezcan a personas que reciben atención médica, cuyo nivel de riesgo es medio y de categoría especial.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	Los titulares de los datos personales sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable. En caso de las brigadas de calle los datos personales son obtenidos en la vía pública.	Recabar información para formar un expediente con base a la recepción de solicitudes de refugio para dormir, de apoyo humanitario en calle con alimentos, cobijas, impermeables; de solicitud de derivación a albergue privado; solicitud de estancia temporal con atención de salud, alimentos, de educación y psicológica; solicitud de estancia nocturna con atención médica, de trabajo social, de atención psicológica, regularización académica y de apoyos asistenciales mediante entrega de kit de higiene, de calzado y cobija, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con el artículo 189 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	

Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.
Divulgación	**Remisiones**: Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O, así como para la publicación de padrones de beneficiarios. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** En el caso de personas que requieran canalización a albergues privados: **1.-** A terceros con los cuales el Organismo celebre convenios de colaboración para la guarda y cuidado de estas personas, mismos que asumen el carácter de "encargados", por lo que solo realizan las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de los mismos y limitan su actuación a los términos fijados por este Organismo en su calidad de "responsable". Esta relación entre el responsable y el encargado, se formaliza mediante contrato, convenio o instrumento jurídico, en cuyo clausulado el encargado de obliga a: a).- Realizar el tratamiento de los datos personales conforme a las instrucciones que se le den; b).- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas; c).- Informar a este Organismo cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; d).- Guardar confidencialidad respecto de los datos personales tratados; e).- 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); f).- Abstenerse de transferir los datos personales salvo que el responsable así lo determine; la comunicación derive de una subcontratación y medie la autorización expresa de este Organismo; o por mandato expreso de la autoridad competente; **2.-** De manera interinstitucional, se realizan hacia sujetos obligados que tienen el carácter de "responsables" tales como Hospitales Civiles de Guadalajara y OPD Servicios de Salud Jalisco, para brindar atención médica especial que sea necesaria; al Sistema DIF Jalisco y a los 125 Sistemas DIF Municipales del Estado de Jalisco, a fin de que brinden el apoyo asistencial correspondiente, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, o bien por corresponder a su competencia territorial. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Este Departamento, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.

El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Jefe(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Dirección del Área de Salud y Bienestar
Administrador de Archivos y base de datos	**Nombre**	Alfredo García Valderrama
	Cargo	Director del Área de Salud y Bienestar
	Adscripción	Coordinación de Operación del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Alfredo García Valderrama. Director del Área	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo y en caso de proceder, brinde autorización y validez con su firma.
Jorge Robles Alcorchas. Jefatura del Departamento Médico	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de atención médica o de expedición de certificado médico, integración de expedientes, análisis y seguimiento hasta su conclusión.
Mariana Soto González. Jefatura del Departamento de Nutrición	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de apoyo para otorgar alimentos en modalidad caliente o fría, dotaciones alimentarias mensuales en cualquier modalidad, o para acceder a lactarios, integración de expedientes, análisis y seguimiento hasta su conclusión.
Griselda Ramírez Zarazúa. Jefatura del Departamento de Salud Bucal	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de atención odontológica o bucal y de prótesis maxilofacial, integración de expedientes, análisis y seguimiento hasta su conclusión.
Karla Berenice Ramírez Morán. Jefatura del Departamento de Psicología	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de atención psicológica individual, familiar, de pareja, y/o ingreso a escuela de padres y madres, integración de expedientes, análisis y seguimiento, hasta su conclusión.
Elba Araceli Gallo Vázquez. Jefatura del Departamento de Laboratorio	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de elaboración de pruebas de laboratorio biológicas, serológicas, bacteriológicas, prematrimoniales, inmunológicas, hematológicas, de dengue, de influenza y COVID, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, firma, clave única de registro de población (CURP), fotografía.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo en datos personales de personas mayores de edad y consecuentemente son de categoría estándar. Los datos personales pertenecientes a niñas, niños y adolescentes, son de categoría especial y tienen un nivel de riesgo medio.
Datos sobre la salud: expediente clínico de cualquier atención médica, historial clínico clínico o médico (resultados laboratoriales), referencias o descripción de sintomatologías, detección de enfermedades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, estado físico o mental de la persona, así como la información sobre la vida sexual.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo en datos personales de personas mayores de edad y consecuentemente son de categoría estándar. Los datos personales pertenecientes a niñas, niños y adolescentes, son de categoría especial y tienen un nivel de riesgo medio, al tratarse de datos personales sensibles.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Los titulares de los datos personales o representantes o tutores de los menores de edad, sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo del programa o servicio asistencial y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con los artículos 116, 118, 120, 122 y 124 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.	
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de la siguiente manera: 1.- A terceros que tengan el carácter de proveedores de bienes o servicios de este Organismo, estrictamente para dar seguimiento a la solicitud de apoyo, mismos que asumen el carácter de "encargados", por lo que solo realizan las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de los mismos y limitan su actuación a los términos fijados por este Organismo en su calidad de "responsable". Esta relación entre el responsable y el encargado, se formaliza mediante contrato, convenio o instrumento jurídico, en cuyo clausulado el encargado de obliga a: a).- Realizar el tratamiento de los datos personales conforme a las instrucciones que se le den; b).- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas; c).- Informar a este Organismo cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; d).- Guardar confidencialidad respecto de los datos personales tratados; e).- 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); f).- Abstenerse de transferir los datos personales salvo que el responsable así lo determine; la comunicación derive de una subcontratación y medie la autorización expresa de este Organismo; o por mandato expreso de la autoridad competente; 2.- Se realizan de manera interinstitucional, al OPD Servicios de Salud Jalisco, Hospitales Civiles de Guadalajara, para dar seguimiento en la atención cuando así se requiera. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf	
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.	
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.	
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.	
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.	
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** En esta Dirección, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.	

El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Dirección del Área Trabajo Social
Administrador de Archivos y base de datos	**Nombre**	Dora Aida Vargas Ocegueda
	Cargo	Directora del Área de Trabajo Social
	Adscripción	Coordinación de Operación del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Dora Aida Vargas Ocegueda. Directora del Área	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de apoyo, integración de expedientes, análisis, seguimiento, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo y en caso de proceder, brinde autorización y validez con su firma.
Nombre. *(vacante)* Jefatura del Departamento de Trabajo Social	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de apoyo, integración de expedientes, análisis y seguimiento, respecto a Trabajo Social.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, teléfono particular, teléfono celular, firma, clave única de registro de población (CURP), clave de elector, lugar y fecha de nacimiento, nacionalidad, edad, estado civil, fotografía, y huella digital.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo. Los datos personales son de categoría estándar a excepción de la huella dactilar que es un dato personal sensible
Datos sobre la salud: expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, discapacidades, intervenciones quirúrgicas, consumo de medicamentos, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, estado físico o mental de la persona, grupo sanguíneo.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo. Los datos personales son sensibles
Datos laborales: Referencias laborales.	Directa/Presencial	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos patrimoniales: Los correspondientes a bienes muebles e inmuebles, vehículos automotores, adeudos, ingresos y egresos y dependencia económica.	Directa/Presencial	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos académicos: Trayectoria educativa.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	Los titulares de los datos personales o representantes o tutores de los menores de edad, sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo del programa o servicio asistencial y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con el artículo 111 del Reglamento Interno de este Organismo.

Almacenamiento	2.eliminado
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial y en caso de proceder, se brinde el mismo.
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de la siguiente manera: **1.-** A terceros que tengan el carácter de proveedores de bienes o servicios de este Organismo, estrictamente para dar seguimiento a la solicitud de apoyo, mismos que asumen el carácter de "encargados", por lo que solo realizan las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de los mismos y limitan su actuación a los términos fijados por este Organismo en su calidad de "responsable". Esta relación entre el responsable y el encargado, se formaliza mediante contrato, convenio o instrumento jurídico, en cuyo clausulado el encargado de obliga a: **a).-** Realizar el tratamiento de los datos personales conforme a las instrucciones que se le den; **b).-** Abstenerse de tratar los datos personales para finalidades distintas a las instruidas; **c).-** Informar a este Organismo cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; **d).-** Guardar confidencialidad respecto de los datos personales tratados; **e).-** 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);* **f).-** Abstenerse de transferir los datos personales salvo que el responsable así lo determine; la comunicación derive de una subcontratación y medie la autorización expresa de este Organismo; o por mandato expreso de la autoridad competente; **2.-** De manera interinstitucional, se realizan hacia autoridades que tienen el carácter de "responsables" tales como el Sistema DIF Jalisco, los 125 Sistemas DIF Municipales del Estado de Jalisco, a fin de que brinden el apoyo asistencial correspondiente, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, o bien por corresponder a su competencia territorial. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** En esta Dirección, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.

El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Dirección del Área de Habilidades y Desarrollo Comunitario
Administrador de Archivos y base de datos	**Nombre**	Andrés Williams Romo de Viviar
	Cargo	Director del Área de Habilidades y Desarrollo Comunitario
	Adscripción	Coordinación de Operación del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Andrés Williams Romo de Vivar. Director del Área	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo y en caso de proceder, brinde autorización y validez con su firma.
Jorge Luis Zacarias Robles. Jefatura del Departamento de Desarrollo Comunitario	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de apoyo de atención psicológica y de atención médica, integración de expedientes, análisis y seguimiento hasta su conclusión.
Lázaro Jorge Luis Sánchez Morlett. Jefatura del Departamento de Educación Extraescolar	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de apoyo en admisión a talleres o adiestramientos, integración de expedientes, análisis y seguimiento hasta su conclusión.
Ameyalli Covarrubias Cueva. Jefatura del Departamento de Comedores Comunitarios	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de apoyo de ración alimenticia en los comedores comunitarios, integración de expedientes, análisis y seguimiento hasta su conclusión.
Nicté Araceli del Muro Anaya. Jefatura del Departamento de Educación Preescolar	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de apoyo de admisión a educación preescolar, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, firma, clave única de registro de población (CURP), fotografía.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo en datos personales de personas mayores de edad y consecuentemente son de categoría estándar. Los datos personales pertenecientes a niñas, niños y adolescentes, son de categoría especial.
Datos sobre la salud: Historial clínico o médico (resultados laboratoriales)	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo en datos personales de personas mayores de edad y consecuentemente son de categoría estándar. Los datos personales pertenecientes a niñas, niños y adolescentes, son de categoría especial y tienen un nivel de riesgo medio, al tratarse de datos personales sensibles.
Datos patrimoniales: Los correspondientes ingresos, egresos y dependencia económica.	Directa/Presencial	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.

Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	Los titulares de los datos personales o representantes o tutores de los menores de edad, sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo del programa o servicio asistencial y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con los artículos 138, 140, 142 y 144 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	

Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de manera interinstitucional, a la Secretaría de Educación Jalisco, en el caso de alumnos de preescolar para la validez oficial del certificado de estudios, así como al Sistema DIF Jalisco, en los casos de apoyo de raciones alimenticias para comprobación de la aplicación de los recursos. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** En esta Dirección, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

:s

...sin embargo, hoy en día, fue cambiado el archivo de concentración a otra área segura y sin este tipo de problemas.

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)	
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.	
Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo	
6.eliminado	
Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado
A fin de lograr el debido tratamiento y protecció Unidad de Transparencia, con la coordinación y siguientes capacitaciones y actualizaciones al p **establecidos en la Ley de protección de los** principios de licitud, finalidad, lealtad, consentim datos personales, así como los deberes que tie **de protección de Datos personales.** Objetivo conocer los pasos para implementación de un S documento de Seguridad. **Tercer trimestre: Av** contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.	
Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Dirección del Área de Centros de Atención Infantil
Administrador de Archivos y base de datos	**Nombre**	Rosa María Guzmán Torres
	Cargo	Director del Área de Centros de Atención Infantil
	Adscripción	Coordinación de Operación del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Rosa María Guzmán Torres. Director del Área	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo y en caso de proceder, brinde autorización y validez con su firma.
Ángeles María Fuentes Larios. Jefatura del Departamento de Nutrición de CDI, CAIC y CEDI	Uso	Conservación y mejora del estado físico nutricional de niñas y niños que asisten a los Centros, análisis y seguimiento hasta su conclusión en cada ciclo.
Ramón Barbarin Vázquez. Jefatura del Departamento de Educación Física y Deportes	Uso	Conservación y mejora del estado físico de niñas y niños que asisten a los Centros para prevenir factores de riesgo de salud, análisis y seguimiento hasta su conclusión.
Ana María Basabilbaso Medina. Jefatura del Departamento de CDI, CAIC y CEDI	Almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de admisión a educación inicial y preescolar, integración de expedientes, análisis y seguimiento, hasta su conclusión.
Barba Gutiérrez Alma Susana. Directora CDI 6 Nancy Castillo Miranda. Directora CDI 13 Covarrubias Paz Laura Araceli Directora CDI 08 García Castañeda Miriam Guadalupe. Directora CDI 11 García García Jessica Nayeli. Directora CDI 01 Gómez Meza Mónica. Directora CDI 02 Gutiérrez Salazar Nohemí Edith. Directora CDI 04 Lomelí Mejía Anna Laura. Directora CDI 05 Magaña Ruiz Sonia María Guadalupe. Directora CDI 10 Méndez Alcaraz María Del Carmen. Directora CDI 07 Mercado Cordero Mónica Cristina. Directora CDI 03 Morales Moreno Ma Del Socorro Anavel. Directora CDI 09	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de admisión a educación inicial y preescolar, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, firma, clave única de registro de población (CURP), fotografía, número de teléfono.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo en datos personales de personas mayores de edad y consecuentemente son de categoría estándar. Los datos personales pertenecientes a niñas, niños y adolescentes, son de categoría especial.
Datos sobre la salud: Historial clínico o médico (resultados laboratoriales), cartilla de vacunación, número de seguridad social.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo en datos personales de personas mayores de edad y consecuentemente son de categoría estándar. Los datos personales pertenecientes a niñas, niños y adolescentes, son de categoría especial y tienen un nivel de riesgo medio, al tratarse de datos personales sensibles.
Datos patrimoniales: Los correspondientes a ingresos.	Directa/Presencial	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos laborales: Carta de trabajo, número de seguridad social.	Directa/Presencial	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Los titulares de los datos personales o representantes o tutores de los menores de edad, sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo del programa o servicio asistencial de guardería y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con los artículos 125, 128, 129, 131 y 133 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.	
Divulgación	**Remisiones:** Se remiten los expedientes de manera integra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de manera interinstitucional, a la Secretaría de Educación Jalisco, para la validez oficial del certificado de estudios. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf	
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.	
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.	
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.	
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.	
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** En esta Dirección, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.	
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.	
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.	

Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo	
6.eliminado	
Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Dirección del Área de la Unidad de Protección Civil
Administrador de Archivos y base de datos	**Nombre**	Miguel Ángel Mosqueda Terán
	Cargo	Director del Área de la Unidad de Protección Civil
	Adscripción	Coordinación de Operación del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Miguel Ángel Mosqueda Terán. Director del Área	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo y en caso de proceder, brinde autorización y validez con su firma.
Francisco Javier Santiago Cerecedo. Soporte Omar Soto Talavera. Soporte	Obtención, almacenamiento, uso, divulgación.	Recepción de solicitudes de apoyo para la atención humanitaria a personas que sufrieron afectación por condiciones de emergencia o desastre, así como para asistencia en brigadas nocturnas, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, firma, nacionalidad, edad, fotografía.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo. Los datos personales son de categoría estándar, es decir, no sensibles. Tratándose de datos personales de niñas, niños o adolescentes, su nivel de riesgo es medio y de categoría especial.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	Personal de la adscripción, se traslada al lugar en donde haya acontecido alguna situación de emergencia o desastre natural, para identificar a personas afectadas y también realiza recorridos por las vialidades de la Ciudad para asistencia en brigadas nocturnas para identificar personas en condición de calle. Se entrevista de forma directa a los titulares de los datos personales o representantes o tutores de los menores de edad, sujetos de asistencia social y proporcionan los datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo del programa o servicio asistencial y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con el artículo 146 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.	
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de manera interinstitucional, a la Unidad de Protección Civil y Bomberos de Guadalajara, así como al Sistema DIF Jalisco, para la colaboración y atención conjunta de personas beneficiarias. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf	

Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** En esta Dirección, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

a

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)	
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.	
Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo
6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación
A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Delegación Institucional de la Procuraduría de Protección de Niñas, Niños y Adolescentes
Administrador de Archivos y base de datos	**Nombre**	Sandra Paola Trelles Rivas
	Cargo	Delegada Institucional de la Procuraduría de Protección de Niñas, Niños y Adolescentes
	Adscripción	Coordinación de Programas del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Sandra Paola Trelles Rivas. Delegada Institucional de la Procuraduría de Protección de Niñas, Niños y Adolescentes	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de reportes de maltrato infantil y de violencia familiar; de seguimiento a medidas de protección emitidas por la Fiscalía Estatal en favor de Niñas, Niños y Adolescentes, para garantizar la protección y restitución integral de sus derechos; de solicitudes de expedición de certificado de idoneidad para llevar a cabo adopción, así como de solicitudes de expedición de certificado de familia de acogida y en caso de proceder, brinde autorización y validez con su firma.
Giovana Elizabeth Navarro Nava. Jefatura del Departamento de Custodia, Tutela, Adopción y Acogimiento Familiar.	Obtención, almacenamiento, uso, divulgación.	Recepción de solicitudes de expediente de reportes de maltrato infantil; de seguimiento a medidas de protección emitidas por la Fiscalía Estatal en favor de Niñas, Niños y Adolescentes, para garantizar la protección y restitución integral de sus derechos; de solicitudes de expedición de certificado de idoneidad para llevar a cabo adopción, así como de solicitudes de expedición de certificado de familia de acogida, integración de expedientes, análisis y seguimiento hasta su conclusión, brindando autorización y validez con su firma.
María Luisa Barrientos Navarro. Jefatura del Departamento de Unidades de Atención a la Violencia Familiar	Obtención, almacenamiento, uso, divulgación.	Recepción de solicitudes de expediente de reportes de maltrato infantil y de violencia familiar; integración de expedientes, análisis y seguimiento hasta su conclusión, brindando autorización y validez con su firma.
Cinthya Angelica Torres Bravo. Jefatura del Departamento de Representación Jurídica de Niñas, Niños y Adolescentes	Obtención, almacenamiento, uso, divulgación.	Recepción de solicitudes de solicitud de asesoría en materia familiar y de trámite de testamento ológrafo, integración de expedientes, análisis y seguimiento hasta su conclusión, brindando autorización y validez con su firma.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, edad, domicilio, firma, estado civil, fotografía.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor, o por la autoridad ministerial que lo pone a disposición).	El nivel de riesgo es bajo en datos personales de personas mayores de edad y consecuentemente son de categoría estándar. Los datos personales pertenecientes a niñas, niños y adolescentes, son de categoría especial y tienen un nivel de riesgo medio.
Datos sobre la salud: historial clínico o médico, (resultados laboratoriales), detección de enfermedades, consumo de estupefacientes (mediante examen toxicológico), estado físico o mental de la persona.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor, o por la autoridad ministerial que lo pone a disposición).	El nivel de riesgo es bajo en datos personales de personas mayores de edad y consecuentemente son de categoría estándar. Los datos personales pertenecientes a niñas, niños y adolescentes, son de categoría especial y tienen un nivel de riesgo medio, al tratarse de datos personales sensibles.
Datos Laborales: referencias laborales, referencias personales.	Directa/Presencial	El nivel de riesgo es bajo y consecuentemente son de categoría estándar.
Datos Patrimoniales: Los correspondientes a bienes muebles e inmuebles, ingresos y egresos, dependientes económicos.	Directa/Presencial	El nivel de riesgo es bajo y consecuentemente son de categoría estándar.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	Los titulares de los datos personales o representantes o tutores de los menores de edad, sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable. En los casos de niñas, niños o adolescentes puestos a disposición los datos personales se obtienen a través de la autoridad ministerial que lo pone a disposición).	Recabar información para formar un expediente con base a un reportes de maltrato infantil y de violencia familiar; o bien; para dar de seguimiento a medidas de protección emitidas por la Fiscalía Estatal en favor de Niñas, Niños y Adolescentes, para garantizar la protección y restitución integral de sus derechos; con base a solicitudes de expedición de certificado de idoneidad para llevar a cabo adopción, así como de solicitudes de expedición de certificado de familia de acogida y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con los artículos 152 al 160 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial, o para la atención de reportes de maltrato infantil y de violencia familiar; de seguimiento a medidas de protección emitidas por la Fiscalía Estatal en favor de Niñas, Niños y Adolescentes, para garantizar la protección y restitución integral de sus derechos; de solicitudes de expedición de certificado de idoneidad para llevar a cabo adopción, asi como de solicitudes de expedición de certificado de familia de acogida	
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de la siguiente manera: 1.- A terceros que tengan el carácter de proveedores de bienes o servicios de este Organismo, estrictamente para proporcionar o brindar el bien o el servicio requerida; de igual forma a terceros que tengan el carácter de "Colaboradores" del Organismo, en aquellos casos en que brinde apoyo de albergue para niñas, niños o adolescentes, mismos que asumen el carácter de "encargados", por lo que solo realizan las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de los mismos y limitan su actuación a los términos fijados por este Organismo en su calidad de "responsable". Esta relación entre el responsable y el encargado, se formaliza mediante contrato, convenio o instrumento jurídico, en cuyo clausulado el encargado de obliga a: a).- Realizar el tratamiento de los datos personales conforme a las instrucciones que se le den; b).- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas; c).- Informar a este Organismo cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; d).- Guardar confidencialidad respecto de los datos personales tratados; e).- 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); f).- Abstenerse de transferir los datos personales salvo que el responsable así lo determine; la comunicación derive de una subcontratación y medie la autorización expresa de este Organismo; o por mandato expreso de la autoridad competente; 2.- Se realizan de manera interinstitucional, a las autoridades judiciales locales o federales, con la finalidad de dar trámite a los juicios correspondientes o para el cumplimiento de los requerimientos judiciales, la Fiscalía del Estado de Jalisco mediante la presentación de denuncias o querellas o cumplir sus requerimientos, a los Sistemas DIF Municipales o al Sistema DIF Jalisco, para derivar asuntos que sean de su competencia o para que atienda solicitudes de apoyo y colaboración. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf	
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.	
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.	
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.	
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.	

Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Esta Delegación y sus áreas, no realizan transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Dirección del Área de Atención Humanitaria
Administrador de Archivos y base de datos	**Nombre**	Fernando Tolentino de la Mora
	Cargo	Director del Área de Atención Humanitaria
	Adscripción	Coordinación de Programas del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Fernando Tolentino de la Mora. Director del Área	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo asistencial y en caso de proceder, brinde autorización y validez con su firma.
Ma. Luisa Cuellar López. Coordinador de Proyecto Rebeca Selene Velázquez Murua. Soporte Verónica Lizeth Cuevas Vázquez. Soporte	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de apoyo y atención psicológica y psicosocial a familiares directos de personas desaparecidas, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, clave única de registro de población (CURP), edad, fotografía, clave de elector, número de pasaporte.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo. Los datos personales son de categoría estándar a excepción de los datos personales de niñas, niños o adolescentes, cuyo nivel de riesgo es medio y de categoría especial.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	Los titulares de los datos personales o representantes o tutores de los menores de edad, sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo para atención psicológica y psicosocial a familiares directos de personas desaparecidas y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con los artículos 166 y 167 fracción XXVI del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.	
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O, así como el para la publicación de padrones de beneficiarios en el portal de Transparencia. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de manera interinstitucional, es decir, hacia autoridades que tienen el carácter de "responsables", tal como lo es el Gobierno Municipal de Guadalajara y el Sistema DIF Jalisco, a fin de que briden servicios de asistencia social, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf	

Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Esta Dirección, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo	
6.eliminado	
Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Departamento de Casa Hogar Villas Miravalle
Administrador de Archivos y base de datos	**Nombre**	Ivonne Aidee Casillas Corona
	Cargo	Jefa de Departamento de Casa Hogar Villas Miravalle
	Adscripción	Dirección del Área de Atención Humanitaria de la Coordinación de Programas del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Ivonne Aidee Casillas Corona. Jefa de Departamento de Casa Hogar Villas Miravalle	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en los expedientes de niñas, niños y adolescentes puestos a disposición de la Delegación Institucional de la PPNNA y en caso de proceder su ingreso al albergue, brinde autorización y validez con su firma, dando un seguimiento para que reciban atención multidisciplinaria por profesionistas en psicología, nutrición, trabajo social, odontología y medicina pediátrica, seguimiento de reintegración educativa y de capacitación para el trabajo, durante su estancia, hasta su egreso y conclusión.
Juan José Alvarado Razo. Jefe de Turno Mónica Elizabeth Jara Avalos. Coordinador de Proyecto María Isabel Herrera Ortiz. Supervisor Aida Araceli Macías Ruvalcaba. Supervisor Eduardo Manuel Alcaraz García. Supervisor	Obtención, almacenamiento, uso, divulgación.	Recepción de solicitudes de apoyo y atención de niñas, niños y adolescentes puestos a disposición de la Delegación Institucional de la PPNNA *(por ser posibles víctimas de algún ilícito penal)* y proporcionar atención multidisciplinaria por profesionistas en psicología, nutrición, trabajo social, odontología y medicina pediátrica; reintegración educativa y de capacitación para el trabajo, durante su estancia, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, clave única de registro de población (CURP), edad, fotografía.	Indirecta/Presencial (al tratarse de caso de niñas, niños o adolescentes, puestos a disposición, los datos personales se obtienen de manera indirecta/presencial por conducto de quien ejercerá la representación en suplencia de la Delegación Institucional de Niñas, Niños o Adolescentes).	El nivel de riesgo es medio. Los datos personales son de categoría estándar por corresponder a niñas, niños o adolescentes, puestos a disposición por ser posibles víctimas de algún ilícito penal y por ende son de categoría especial.
Datos sobre la salud: Historial clínico o médico	Indirecta/Presencial (al tratarse de caso de niñas, niños o adolescentes, puestos a disposición, los datos personales se obtienen de manera indirecta/presencial por conducto de quien ejercerá la representación en suplencia de la Delegación Institucional de Niñas, Niños o Adolescentes).	El nivel de riesgo es medio. Los datos personales son de categoría estándar por corresponder a niñas, niños o adolescentes, puestos a disposición por ser posibles víctimas de algún ilícito penal y por ende son de categoría especial y por corresponder a datos de su salud.
Datoss académicos: Trayectoria educativa, avances de créditos, promedio, calificaciones.	Indirecta/Presencial (al tratarse de caso de niñas, niños o adolescentes, puestos a disposición, los datos personales se obtienen de manera indirecta/presencial por conducto de quien ejercerá la representación en suplencia de la Delegación Institucional de Niñas, Niños o Adolescentes).	El nivel de riesgo es medio. Los datos personales son de categoría estándar por corresponder a niñas, niños o adolescentes, puestos a disposición por ser posibles víctimas de algún ilícito penal y por ende son de categoría especial.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Los funcionarios públicos que ejercen la representación en suplencia de las niñas, niños o adolescentes sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo para atención de niñas, niños y adolescentes puestos a disposición de la Delegación Institucional de la PPNNA (por ser posibles víctimas de algún ilícito penal) y proporcionar atención multidisciplinaria por profesionistas en psicología, nutrición, trabajo social, odontología y medicina pediátrica; reintegración educativa y de capacitación para el trabajo, durante su estancia, y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con los artículos 169 y 170 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.	
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O, así como el para la publicación de padrones de beneficiarios en el portal de Transparencia. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de manera interinstitucional, es decir, hacia autoridades que tienen el carácter de "responsables", tales como el Sistema DIF Jalisco, los 125 Sistemas DIF Municipales del Estado de Jalisco y la Secretaría de Educación Jalisco a fin de que briden servicios de asistencia social o de admisión en los centros educativos y de reconocimiento oficial de estudios, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf	
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.	
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.	
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.	
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.	
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Este Departamento, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.	
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.	

Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Departamento de Prevención, Atención y Acompañamiento de Niñas, Niños y Adolescentes
Administrador de Archivos y base de datos	**Nombre**	Jorge Arturo Ávila Cervantes
	Cargo	Jefe del Departamento de Prevención, Atención y Acompañamiento de Niñas, Niños y Adolescentes
	Adscripción	Dirección del Área de Derechos de la Niñez de la Coordinación de Programas del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Jorge Arturo Ávila Cervantes. Jefe de Departamento	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de apoyo asistencial y en caso de proceder, brinde autorización y validez con su firma.
Paulina Flores López. Coordinador de Proyecto Xóchitl Torres Regalado. Coordinador de Proyecto Bayardo Vega Hernández. Coordinador de Proyecto	Obtención, almacenamiento, uso, divulgación.	Recepción de solicitudes de apoyo y atención mediante actividades de promoción de derechos, de psicológica, de atención y seguimiento a niñas, niños y adolescentes en situación de riesgo, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, clave única de registro de población (CURP), edad, fotografía, clave de elector, número de teléfono.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es medio. Los datos personales son de categoría especial por corresponder a datos personales de niñas, niños o adolescentes.
Datos patrimoniales: Los correspondientes a ingresos y egresos.	Directa/Presencial	El nivel de riesgo es medio. Los datos personales son de categoría especial por corresponder a datos personales de niñas, niños o adolescentes.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado Office, con el software de Word y Excel.	

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	Los titulares de los datos personales o representantes o tutores de los menores de edad, sujetos de asistencia social, son invitados o convocados para que acudan de forma presencial y realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo y atención mediante actividades de promoción de derechos, de psicológica, de atención y seguimiento a niñas, niños y adolescentes en situación de riesgo y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con los artículos 164 y 165 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado acceso.	
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.	

Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O, así como el para la publicación de padrones de beneficiarios en el portal de Transparencia. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de manera interinstitucional, es decir, hacia autoridades que tienen el carácter de "responsables", es decir, al Sistema DIF Jalisco, o a los DIF Municipales, a fin de que briden servicios de asistencia social, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Este Departamento, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo	
6.eliminado	
Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Departamento de Atención a Mujeres
Administrador de Archivos y base de datos	**Nombre**	María de los Ángeles González Ramírez
	Cargo	Jefa del Departamento de Atención a Mujeres
	Adscripción	Dirección del Área de Atención Humanitaria de la Coordinación de Programas del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
María de los Ángeles González Ramírez. Jefe de Departamento	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en los expedientes de mujeres víctimas de violencia que sean canalizadas por las Unidades de Atención a la Violencia Familiar del propio DIF Guadalajara; por el Centro Integral de Atención a las Violencias de Guadalajara (CIAV); o por el Centro de Justicia para las Mujeres de la Fiscalía del Estado de Jalisco y en caso de proceder su ingreso al refugio, brinde autorización y validez con su firma, dando un seguimiento para esas mujeres y sus hijos e hijas *(niñas, niños o adolescentes)*, reciban alojamiento, alimentación, atención médica, psicológica, educativa y trabajo social, durante su estancia y hasta su egreso y conclusión.
María de los Ángeles Hernández Pérez. Soporte Margarita del Refugio Cardiel Ramos. Soporte fin de Semana Lizbeth Marisol Cervantes Ramírez. Analista	Obtención, almacenamiento, uso, divulgación.	Recepción de solicitudes de apoyo y atención a mujeres víctimas de violencia que sean canalizadas por las Unidades de Atención a la Violencia Familiar del propio DIF Guadalajara; por el Centro Integral de Atención a las Violencias de Guadalajara (CIAV); por el Centro de Justicia para las Mujeres de la Fiscalía del Estado de Jalisco o por la Secretaría de Igualdad Sustantiva entre Mujeres y Hombres del Gobierno del Estado, para dar un seguimiento para esas mujeres y sus hijos e hijas (niñas, niños o adolescentes), brindando alojamiento, alimentación, atención médica, psicológica, educativa y trabajo social durante su estancia y hasta su egreso.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, domicilio, clave única de registro de población (CURP), edad.	Directa/Presencial (En caso de los datos personales de niñas, niños o adolescentes que acompañen a una mujer víctima de violencia, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor).	El nivel de riesgo es medio. Los datos personales son de categoría estándar por corresponder a mujeres víctimas de violencia familiar, así como de niñas, niños o adolescentes y por ende requieren tratamiento especial.
Datos sobre la salud: Historial clínico o médico	Directa/Presencial (En caso de los datos personales de niñas, niños o adolescentes que acompañen a una mujer víctima de violencia, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor).	El nivel de riesgo es medio. Los datos personales son de categoría estándar por corresponder a mujeres víctimas de violencia familiar, así como de niñas, niños o adolescentes y por ende requieren tratamiento especial.
Datos académicos: Trayectoria educativa, promedio, calificaciones.	Directa/Presencial (En caso de los datos personales de niñas, niños o adolescentes que acompañen a una mujer víctima de violencia, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor).	El nivel de riesgo es medio. Los datos personales son de categoría estándar por corresponder a mujeres víctimas de violencia familiar, así como de niñas, niños o adolescentes y por ende requieren tratamiento especial.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Los titulares de los datos personales que son derivados al refugio o representantes o tutores de los menores de edad que los acompañan, de manera presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo para atención a mujeres víctimas de violencia, para darles un seguimiento a ellas y sus hijos e hijas (niñas, niños o adolescentes), brindando alojamiento, alimentación, atención médica, psicológica, educativa y trabajo social durante su estancia y hasta su egreso, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con los artículos 171 y 172 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.	
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O, así como el para la publicación de padrones de beneficiarios en el portal de Transparencia. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de manera interinstitucional, es decir, hacia autoridades que tienen el carácter de "responsables", tales como el Sistema DIF Jalisco, los 125 Sistemas DIF Municipales del Estado de Jalisco *(por medio de las Unidades de Atención a la Violencia Familiar)*; Gobierno Municipal de Guadalajara; Fiscalía del Estado de Jalisco, Instituto de las Mujeres de Guadalajara y por la Secretaría de Igualdad Sustantiva entre Mujeres y Hombres, a fin de que briden servicios de asistencia social, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf	
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.	
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.	
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.	
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.	
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Este Departamento, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.	

El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. Se tiene prohibido el ingreso a personas no autorizadas.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Departamento de Complejo Sauz
Administrador de Archivos y base de datos	**Nombre**	María Concepción Sánchez López
	Cargo	Jefa de Departamento Complejo Sauz
	Adscripción	Dirección Administrativa del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
María Concepción Sánchez López. Jefatura de Departamento Complejo Sauz	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de solicitudes de admisión a clases de natación, integración de expedientes y en caso de proceder, brinde autorización y validez con su firma, dando seguimiento hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, domicilio, firma, clave única de registro de población (CURP), fotografía.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo en datos personales de personas mayores de edad y consecuentemente son de categoría estándar. Los datos personales pertenecientes a niñas, niños y adolescentes, tienen un nivel de riesgo medio y son de categoría especial.
Datos sobre la salud: Historial clínico o médico (mediante certificado médico)	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo en datos personales de personas mayores de edad y consecuentemente son de categoría estándar. Los datos personales pertenecientes a niñas, niños y adolescentes, tienen un nivel de riesgo medio y son de categoría especial.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Los titulares de los datos personales o representantes o tutores de los menores de edad, sujetos de asistencia social, acuden de forma presencial, realizan el llenado de formularios y entregan documentación con datos personales conforme a los lineamientos, Reglas de Operación, Reglamento o normativa aplicable.	Recabar información para formar un expediente con base a la solicitud de apoyo de admisión a clases de natación y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 5 del Código de Asistencia Social, en relación con el artículo 94 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	

Uso	Se revisa y se coteja la información contenida en el expediente de solicitud de apoyo para el debido desarrollo del servicio asistencial.
Divulgación	**Remisiones:** En este Departamento, no se realizan transferencias de datos personales.
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Considerando que no se realizan transferencias de datos personales, no se hace manifestación al respecto.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Jefe(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo	
6.eliminado	
Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado
A fin de lograr el debido tratamiento y pr…dad, la Unidad de Transparencia, con la coordi…el año las siguientes capacitaciones y actuali…**pios y deberes establecidos en la Ley de pro**…onocer los principios de licitud, finalidad, lealtad…miento de los datos personales, así como los de…**dad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.	
Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Dirección del Área de Recursos Humanos
Administrador de Archivos y base de datos	**Nombre**	Tania Elizabeth Sánchez García
	Cargo	Directora del Área de Atención Humanitaria
	Adscripción	Dirección Administrativa del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Tania Elizabeth Sánchez García. Directora del Área	Uso, divulgación y cancelación.	Análisis de la información y documentación con la que se cuenta en los expedientes personales laborales y bases de datos, brindando autorización y validez con su firma en aquellos casos que sea necesario, así como llevando a cabo su resguardo, para la debida protección de los datos personales.
Delia Beatriz Cárdenas Godínez. Jefatura del Departamento de Reclutamiento, Selección y Contratación	Obtención, almacenamiento, uso, divulgación, cancelación.	Recepción de documentos con datos personales, derivado de altas y bajas de empleados, elaboración de credenciales oficiales a empleados, atención solicitudes de constancias laborales, constancias de baja y de hojas de servicio, trámite de altas y bajas ante el IMSS, registro de incapacidades y atención a riesgos de trabajo, integración de expediente y trámite hasta su conclusión, validando con su antefirma.
Mauricio Iván Fonseca Guerra. Jefatura del Departamento de Incidencias, Capacitación e Inducción	Obtención, almacenamiento, uso, divulgación, cancelación.	Elaboración de curriculum en versiones públicas, recepción y atención de solicitudes de servicio social y prácticas profesionales, registro, trámite y seguimiento de incidencias del personal, integración de expediente y trámite hasta su conclusión y validación con su antefirma.
Alma Deliá de la Torre González. Jefatura del Departamento de Nómina	Obtención, almacenamiento, uso, divulgación, cancelación.	Elaboración y dispersión de nómina, solicitud de trámite de tarjeta de nómina, solicitud de dispersión de vales de despensa, retención de aportaciones al IPEJAL, retención y pago de retenciones a terceros, elaboración de cálculo y pago de finiquitos, cálculo de aportaciones del SEDAR, integración de expediente y trámite hasta su conclusión y validación con su antefirma.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, edad, domicilio, número de teléfono particular o celular, huella digital, tipo de sangre, clave única de registro de población (CURP), fotografía, matrícula del servicio militar nacional, clave de elector, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, correo electrónico personal, firma, clave de Registro Federal de Contribuyentes (RFC).	Directa/Presencial/Indirecta	El nivel de riesgo es bajo. Los datos personales son de categoría estándar.
Datos Laborales: Número de seguridad social, documentos de reclutamiento o selección, nombramiento, incidencia, capacitación, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio.	Directa/Presencial/Indirecta	El nivel de riesgo es bajo. Los datos personales son de categoría estándar.
Datos sobre la salud: El expediente clínico de cualquier atención médica, historial médico, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, estado físico o mental de la persona.	Directa/Presencial/Indirecta	El nivel de riesgo es alto. Los datos personales son de categoría especial por corresponder a la salud.
Datos Patrimoniales: Información fiscal, ingresos y egresos (deudas), número de cuenta bancaria y/o CLABE interbancaria, referencias personales, beneficiarios, dependientes económicos.	Directa/Presencial/Indirecta	El nivel de riesgo es medio. Los datos personales son de categoría estándar.
Datos sobre situación jurídica o legal: La información relativa a una persona que se encuentre o haya sido sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho.	Indirecta	El nivel de riesgo es medio. Los datos personales son de categoría estándar.

Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Los titulares de los datos personales acuden de forma presencial, así como en forma electrónica, realizan el llenado de formularios y entregan documentación con datos personales conforme al Reglamento Interno, o normativa aplicable.	Recabar información para formar un expediente personal laboral o de servicio social o de prácticas y dar un seguimiento a ello hasta su conclusión, de conformidad con los artículos 55 al 63 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	La información se utiliza de forma cotidiana, derivado de la actualización o integración de información o documentación. Las bases de datos son para la elaboración de todo tipo de movimientos administrativos, así como para la elaboración de credenciales oficiales.	
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O, así como para la publicación de nómina, de listado de jubilados y pensionados y de curiculum vitae en el portal de transparencia. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Transferencias: Se realizan de la siguiente manera: 1.- A terceros que tengan el carácter de proveedores de bienes o servicios de este Organismo, estrictamente para dar seguimiento al pago de la nómina y al pago de la prestación de vales de despensa, mismos que asumen el carácter de "encargados", por lo que solo realizan las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de los mismos y limitan su actuación a los términos fijados por este Organismo en su calidad de "responsable". Esta relación entre el responsable y el encargado, se formaliza mediante contrato, convenio o instrumento jurídico, en cuyo clausulado el encargado de obliga a: a).- Realizar el tratamiento de los datos personales conforme a las instrucciones que se le den; b).- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas; c).- Informar a este Organismo cuando ocurra una vulneración a los datos personales que trata por sus instrucciones; d).- Guardar confidencialidad respecto de los datos personales tratados; e).- 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); f).- Abstenerse de transferir los datos personales salvo que el responsable así lo determine; la comunicación derive de una subcontratación y medie la autorización expresa de este Organismo; o por mandato expreso de la autoridad competente; 2.- De manera institucional, se realizan hacia autoridades que tienen el carácter de "responsables" tales como el Instituto de Pensiones del Estado de Jalisco, el Instituto Mexicano del Seguro Social, a la Secretaría de Hacienda y Crédito Público, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, o bien por corresponder a su competencia territorial. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf	
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción, solo de aquellos documentos cuya conservación no sea necesaria.	
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.	
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.	
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.	

Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Esta Dirección, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo.** - Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Departamento de Ingresos
Administrador de Archivos y base de datos	**Nombre**	Ana María Jiménez Ferrer
	Cargo	Jefa del Departamento de Ingresos
	Adscripción	Dirección del Área de Finanzas de la Dirección Administrativa del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
Ana María Jiménez Ferrer. Jefatura del Departamento de Ingresos	Obtención, almacenamiento, uso, divulgación, cancelación.	El titular de los datos personales, acude de manera directa a realizar el pago de cuotas de recuperación respecto a algún programa o servicio ofrecido por el Organismo, o bien, realiza algún donativo económico en favor del propio Organismo, integración de expediente y trámite hasta su conclusión, validando con su firma.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, edad, domicilio, clave de Registro Federal de Contribuyentes (RFC).	Directa/Presencial/Indirecta/ Electrónica	El nivel de riesgo es bajo. Los datos personales son de categoría estándar.
Datos Patrimoniales: número de cuenta bancaria y/o CLABE interbancaria.	Directa/Presencial/Indirecta/ Electrónica	El nivel de riesgo es medio. Los datos personales son de categoría especial.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Los titulares de los datos personales acuden de forma presencial, así como en forma electrónica y realizan el pago de cuotas de recuperación o de donativos económicos, y entregan documentación o datos personales conforme al Reglamento Interno, o normativa aplicable.	Recabar información para formar un expediente de ingresos o de donativos, hasta su conclusión y así transparentar su recepción y destino de recursos públicos, de conformidad con los artículos 67 y 68 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	La información se utiliza de para comprobar pagos de cuotas o donativos efectuados en favor del Organismo	

Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Transferencias: En este Departamento, no se realizan transferencia de datos personales.
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción, solo de aquellos documentos cuya conservación no sea necesaria.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Considerando que, en esta área, no se realizan transferencia de datos personales, no se hace manifestación al respecto.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)	
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.	
Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo	
6.eliminado	
Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación
A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Departamento de Control Presupuestal
Administrador de Archivos y base de datos	**Nombre**	Ana Gabriela Flores Martínez
	Cargo	Jefa del Departamento de Control Presupuestal
	Adscripción	Dirección de Finanzas de la Dirección Administrativa del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
Ana Gabriela Flores Martínez. Jefatura del Departamento de Control Presupuestal	Obtención, almacenamiento, uso, divulgación, cancelación.	Revisión de trámites de pago, comprobantes de gastos y de viáticos, integración de expediente y trámite hasta su conclusión, validando con su antefirma.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, edad, firma, clave de Registro Federal de Contribuyentes (RFC).	Directa/Presencial/Indirecta	El nivel de riesgo es bajo. Los datos personales son de categoría estándar.
Datos Patrimoniales: Información fiscal, número de cuenta bancaria y/o CLABE interbancaria.	Directa/Presencial/Indirecta	El nivel de riesgo es medio. Los datos personales son de categoría estándar.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Los datos personales se obtienen de forma indirecta, cuando las áreas ejecutoras del gasto, ingresan a revisión trámites de egreso para su pago, dando de alta los datos bancarios, conforme al Reglamento Interno, o normativa aplicable.	Recabar información para formar un expediente de trámite de pago, de comprobante de gastos y de viático, hasta su conclusión, de conformidad con los artículos 69 y 70 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	La información se utiliza para la revisión de trámites de pago, comprobantes de gastos y de viáticos.	

Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Se realizan de la siguiente manera: De manera institucional, a la Auditoria Superior del Estado de Jalisco, con el carácter de autoridad "responsables" siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, o bien por corresponder a su competencia territorial. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción, solo de aquellos documentos cuya conservación no sea necesaria.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Esta área, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes fisicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Departamento de Estados Financieros
Administrador de Archivos y base de datos	**Nombre**	David Piña Guevara
	Cargo	Jefe del Departamento de Estados Financieros
	Adscripción	Dirección del Área de Finanzas de lo Dirección Administrativa del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
David Piña Guevara. Jefatura del Departamento de Estados Financieros	Obtención, almacenamiento, uso, divulgación, cancelación.	Revisión de pólizas de ingresos, diario y egresos para la integración del libro diario de operaciones financieras, así como para generar los informes financieros, hasta su conclusión y validación con su antefirma.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, edad, correo electrónico personal, firma, clave de Registro Federal de Contribuyentes (RFC).	Directa/Presencial/Indirecta	El nivel de riesgo es bajo. Los datos personales son de categoría estándar.
Datos Patrimoniales: Información fiscal, número de cuenta bancaria y/o CLABE interbancaria.	Directa/Presencial/Indirecta	El nivel de riesgo es medio. Los datos personales son de categoría estándar.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Los datos personales se obtienen de forma indirecta, cuando las áreas ejecutoras del gasto, envían comprobantes de ingresos y egresos conforme al Reglamento Interno, o normativa aplicable.	Recabar información para formar un expediente sobre pólizas de egreso y de diario, así como de los Estados Financieros, de conformidad con los artículos 71 y 72 del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	La información se utiliza para generar informes financieros, revisar pólizas de ingresos, diario y de egresos y para coadyuvar en la captura de información para la elaboración del primero y segundo avance de gestión financiera y la cuenta pública.	

Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O, así como para la publicación de nómina, de listado de jubilados y pensionados y de curiculum vitae en el portal de transparencia. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Transferencias: Se realizan a la Auditoria Superior del Estado de Jalisco, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, o bien por corresponder a su competencia territorial. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción, solo de aquellos documentos cuya conservación no sea necesaria.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Esta Dirección, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.

Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

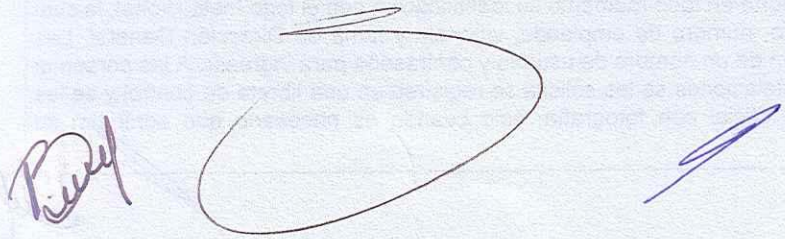
de datos personales.

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024



DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Dirección de Compras y Adquisiciones
Administrador de Archivos y base de datos	**Nombre**	Luisa Elena Fabiola Rodríguez Gómez
	Cargo	Directora del Área de Compras y Adquisiciones
	Adscripción	Dirección Administrativa del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Luisa Elena Fabiola Rodríguez Gómez. Directora del Área	Uso, cancelación.	Análisis, estudio y revisión de expedientes del padrón de proveedores, así como de procesos de licitación y en su caso, autorización con su firma.
Martha Leticia Márquez Tapia. Jefe de Departamento de Cotizadores Ricardo Sandoval Bustos. Soporte	Obtención, almacenamiento, uso, divulgación.	Recepción de documentos con datos personales, derivado de procesos de licitación en cuanto a la etapa de presentación de propuestas técnicas y económicas de cada licitante, así como los datos personales requeridos para causar alta en el padrón de proveedores.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, edad, domicilio fiscal, número de teléfono, clave única de registro de población (CURP), fotografía, clave de elector, lugar y fecha de nacimiento, nacionalidad, correo electrónico, firma, clave de Registro Federal de Contribuyentes (RFC).	Directa/Presencial/Indirecta/electrónica	El nivel de riesgo es bajo. Los datos personales son de categoría estándar.
Datos Patrimoniales: número de cuenta bancaria y/o CLABE interbancaria.	Directa/Presencial/Indirecta	El nivel de riesgo es medio. Los datos personales son de categoría estándar.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	A través de la inscripción, actualización y modificación al padrón de proveedores, se solicitan de manera presencial, documentos y datos personales de personas físicas o morales que tengan intención de vender algún producto, bien o servicio al Organismo. También se solicitan a los proveedores, datos personales y documentos que los contienen, en los procesos de licitación al momento de la presentación de propuestas técnicas y económicas, como parte de los requisitos para su participación, acorde a las bases de licitación.	Recabar información para formar un expediente y tener la certeza de que el proveedor se encuentra debidamente constituido, legal y fiscalmente, es decir, que está al corriente en sus obligaciones fiscales y que por ende, puede ofrecer sus bienes o servicios de manera eficiente, de conformidad con el Reglamento Interno de Adquisiciones, enajenaciones, arrendamientos y contrataciones de bienes o servicios para el OPD, en relación con los artículos 86 y 86 del Reglamento Interno de este Organismo.

Almacenamiento	2.eliminado
Uso	El expediente del padrón de proveedores, una vez que está inscrito se sube al sistema, se elabora versión pública para darle publicidad en el portal de Transparencia. En cuanto al proceso de licitación, existe una etapa de apertura y presentación de propuestas, en la cual se reciben mediante sobre cerrado, las propuestas técnicas y económicas de cada proveedor participante, (las cuales contienen datos personales), mismas que se abren en presencia del personal de la Contraloría Interna, se hace análisis de la información para posteriormente emitir un fallo conforme a los requisitos presentados, precio, condiciones de entrega etc.
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O, así como para la publicación de padrón de proveedores, adjudicaciones directas y procesos de licitación, en el portal de transparencia. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos o en los casos en que se practiquen auditorias o visitas de inspección. **Transferencias:** Transferencias: Se realizan únicamente cuando deriva de un requerimiento por parte de una autoridad judicial, pudiendo ser el Tribunal Administrativo del Estado de Jalisco, Juzgados de Distrito en materia Administrativa, Civil y del Trabajo, la Auditoria Superior del Estado de Jalisco, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, o bien por corresponder a su competencia territorial. Lo anterior conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción, solo de aquellos documentos cuya conservación no sea necesaria.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** Esta Dirección, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.

Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Dirección Jurídica (Pláticas Prematrimoniales)
Administrador de Archivos y base de datos	**Nombre**	José Antonio Castañeda Castellanos.
	Cargo	Director Jurídico
	Adscripción	Dirección Jurídica del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
José Antonio Castañeda Castellanos. Director Jurídico	Uso, cancelación.	Cotejo de los documentos en su totalidad, para su autorización y validez con su antefirma.
Eduardo Ezequiel Camacho Castro. Asimilado a salario	Obtención, almacenamiento, uso, divulgación.	Recepción de peticiones/solicitudes para expedición de constancia de pláticas prematrimoniales, integración de expediente y proyectar resolución.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, firma, clave única de registro de población (CURP), Registro Federal de Contribuyentes (RFC), lugar y fecha de nacimiento, nacionalidad, edad, estado civil.	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos patrimoniales: cuenta bancaria y CLABE interbancaria.	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	Descripción	Finalidad del Tratamiento
Obtención:	A través de la presentación física o electrónica de documentos con datos personales para la expedición de constancia prematrimonial.	Recabar información para formar un expediente con base a una petición y dar seguimiento hasta su conclusión, de conformidad con el artículo 97 fracción XIV del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Cotejo de la totalidad de documentos para la expedición de constancia prematrimonial.	

Divulgación	**Remisiones:** Se remiten de forma íntegra a la Unidad de Transparencia por motivo de solicitudes de información o de ejercicio de derechos ARCO. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos. **Transferencias:** No se realizan transferencias.
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Considerando que no se realizan transferencias de datos personales, no aplica el presente rubro.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)	
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.	
Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo	
6.eliminado	
Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado
Programa General de capacitación	
A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.	
Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Dirección Jurídica (Jefatura del Departamento de Jurídico Consultivo)
Administrador de Archivos y base de datos	**Nombre**	José Antonio Castañeda Castellanos.
	Cargo	Director Jurídico
	Adscripción	Dirección Jurídica del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
José Antonio Castañeda Castellanos. Director Jurídico	Uso, cancelación.	Cotejo de los expedientes en su totalidad, para su autorización y validez con su antefirma.
Erick Antonio Beltrán Prado. Jefe del Departamento de Jurídico Consultivo	Obtención, almacenamiento, uso, divulgación.	Recepción de memorándums con peticiones/solicitudes para elaboración de convenios, contratos y demás instrumentos jurídicos, integración de expediente y elaboración de los proyectos de los antes citados.
Iván Alejandro Palacios Meza. Soporte	Obtención, almacenamiento, uso, divulgación.	Recepción de memorándums con peticiones/solicitudes para elaboración de convenios, contratos y demás instrumentos jurídicos, integración de expediente y elaboración de los proyectos de los antes citados.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, domicilio, firma, clave única de registro de población (CURP), Registro Federal de Contribuyentes (RFC), lugar y fecha de nacimiento, nacionalidad, edad, estado civil.	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos patrimoniales: Información fiscal, número de cuenta bancaria y/o CLABE interbancaria.	Directa/Presencial	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	A través de la presentación física o electrónica de documentos con datos personales para la elaboración de contratos, convenios o instrumentos jurídicos.	Recabar información para formar un expediente con base a una petición y dar seguimiento hasta su conclusión, de conformidad con el artículo 97 fracción II del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Cotejo de la totalidad de documentos para la elaboración de contratos, convenios y demás instrumentos jurídicos.	

Divulgación	**Remisiones:** Se remiten de forma íntegra a la Unidad de Transparencia por motivo de solicitudes de información o de ejercicio de derechos ARCO, así como para el cotejo de clasificación inicial de información confidencial previo a su publicación en versión pública en el portal de Transparencia. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos. **Transferencias:** No se realizan transferencias.
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Considerando que no se realizan transferencias de datos personales, no aplica el presente rubro.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Jefe(a) de Departamento en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo	
6.eliminado	
Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado
Programa General de capacitación	
A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.	
Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Dirección Jurídica (Jefatura del Departamento de Jurídico Contencioso)
Administrador de Archivos y base de datos	**Nombre**	José Antonio Castañeda Castellanos.
	Cargo	Director Jurídico
	Adscripción	Dirección Jurídica del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
José Antonio Castañeda Castellanos. Director Jurídico	Uso, cancelación.	Cotejo de los expedientes en su totalidad, para su autorización y validez con su antefirma.
Natanael Nuño Rojas. Jefe del Departamento de Jurídico Contencioso.	Obtención, almacenamiento, uso, divulgación.	Recepción de memorándum con solicitudes, integración de expediente y análisis del mismo para proyectar una resolución en cada caso en particular, en que el DIF Guadalajara sea parte, para la debida defensa de sus intereses ante los Órganos jurisdiccionales en cualquier materia, no jurisdiccionales y autoridades administrativas. De igual forma, para inicio y desahogo de procedimientos de responsabilidad laboral.
Juan Salvador García Aguilar. Soporte	Obtención, almacenamiento, uso, divulgación.	Recepción de memorándum con solicitudes, integración de expediente y análisis del mismo para proyectar una resolución en cada caso en particular, en que el DIF Guadalajara sea parte, para la debida defensa de sus intereses ante los Órganos jurisdiccionales en cualquier materia, no jurisdiccionales y autoridades administrativas. De igual forma, para inicio y desahogo de procedimientos de responsabilidad laboral.
Luis Arturo García Silva. Soporte	Obtención, almacenamiento, uso, divulgación.	Recepción de memorándum con solicitudes, integración de expediente y análisis del mismo para proyectar una resolución en cada caso en particular, en que el DIF Guadalajara sea parte, para la debida defensa de sus intereses ante los Órganos jurisdiccionales en cualquier materia, no jurisdiccionales y autoridades administrativas. De igual forma, para inicio y desahogo de procedimientos de responsabilidad laboral.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, domicilio.	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos laborales: nombramiento.	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos ideológicos: afiliación sindical	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es medio. Los datos personales son sensibles.
Datos sobre situación jurídica o legal: La información relativa a una persona que se encuentre o haya sido sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho,	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos académicos: Cédula profesional.	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	A través de la recepción física o electrónica de escritos de demanda y acuerdos que contienen requerimientos judiciales en cualquier materia, emanados de las autoridades jurisdiccionales o bien requerimientos de Organismos no jurisdiccionales. Finalmente, mediante la recepción de actas circunstanciadas, para inicio de un procedimiento de responsabilidad laboral.	Recabar información para formar un expediente con base a una petición y dar seguimiento hasta su conclusión, de conformidad con el artículo 103 fracciones I a la IX del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Cotejo y estudio de la totalidad de las constancias de los expedientes, para seguir una estrategia jurídica de defensa de los intereses del Organismo.	
Divulgación	**Remisiones:** Se remiten de forma íntegra a la Unidad de Transparencia por motivo de solicitudes de información o de ejercicio de derechos ARCO. Asimismo, se remiten a la Dirección del Área de Recursos Humanos solicitando información laboral cuando se trata de un juicio laboral. De acuerdo a los laudos correspondientes, se remiten a la Dirección del Área de Finanzas para cubrir el pago de las prestaciones a que haya sido condenado el Organismo. **Transferencias:** Se transfiere información con datos personales a las autoridades jurisdiccionales competentes, Fiscalía del Estado de Jalisco, Fiscalía Especializada en Combate a la Corrupción del Estado de Jalisco, así como a la Comisión Estatal de Derechos Humanos, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf	
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.	
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.	
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.	
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.	
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: Transferencias mediante el traslado de soportes físicos: a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. Transferencias mediante el traslado físico de soportes electrónicos: No realizan transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. Transferencias mediante el traslado sobre redes electrónicas: a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.	

El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Jefe (a) del Departamento en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Dirección Jurídica (Centro de convivencia)
Administrador de Archivos y base de datos	**Nombre**	José Antonio Castañeda Castellanos.
	Cargo	Director Jurídico
	Adscripción	Dirección Jurídica del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
José Antonio Castañeda Castellanos. Director Jurídico	Uso, cancelación.	Cotejo de los expedientes en su totalidad, para su autorización y validez con su antefirma.
Ma. Guadalupe Vargas Castro. Jefa del Departamento de Centro de Convivencia.	Obtención, almacenamiento, uso, divulgación.	Recepción de oficios derivados por la autoridad jurisdiccional o por los Centros de Justicia Alternativa en donde se ordena temporalmente una convivencia supervisada o de entrega recepción, integración de expediente, análisis y resolución de conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, domicilio, firma, clave única de registro de población (CURP), lugar y fecha de nacimiento, nacionalidad, edad, estado civil.	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos sobre la salud: referencias o descripción de sintomatologías.	Directa/Presencial	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos sobre situación jurídica o legal: La información relativa a una persona que se encuentre o haya sido sujeta a un procedimiento jurisdiccional en materia familiar.	Directa/Presencial	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	A través de la presentación física o electrónica de documentos con datos personales en donde se ordena convivencia asistida o de entrega-recepción.	Recabar información para formar un expediente con base a una orden y dar seguimiento hasta su conclusión, de conformidad con los artículos 104 y 105 fracciones I a VI del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	

Uso	Cotejo de la totalidad de documentos para la elaboración de informes, a la autoridad jurisdiccional o a los Centros de Justicia Alternativa ordenadora.
Divulgación	**Remisiones:** Se remiten de forma íntegra a la Unidad de Transparencia por motivo de solicitudes de información o de ejercicio de derechos ARCO, así como para el cotejo de clasificación inicial de información confidencial. Asimismo se remiten a la Contraloría Interna, en caso de quejas o denuncias presentadas por ciudadanos, en contra del personal del Centro, en donde se presuma alguna responsabilidad administrativa. **Transferencias:** Se transfiere información con datos personales a las autoridades jurisdiccionales competentes , así como a los Centros de Justicia Alternativa, en su calidad de ordenadoras, siempre y cuando dichas transferencias de datos personales, sean necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Medidas de seguridad administrativas: Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. Medidas de seguridad físicas: Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. Medidas de seguridad técnicas: Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Jefe(a) del Departamento en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos
3.eliminado

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)	
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.	
Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.

Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Área de Planeación, Evaluación y Monitoreo
Administrador de Archivos y base de datos	**Nombre**	Irving Darío Castillo Cisneros
	Cargo	Titular del Área de Planeación, Evaluación y Monitoreo
	Adscripción	Dirección General del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
Irving Darío Castillo Cisneros. Titular del Área	Uso, cancelación.	Revisión, cotejo y estudio de la información contenida en el expediente de solicitud de evaluaciones de calidad de programas y servicios, autorización y validez con su firma.
José Jairo Alvarado Cisneros. Jefe de Departamento de Planeación, Evaluación y Monitoreo	Obtención, almacenamiento, uso.	Recepción de solicitudes de apoyo para practicar evaluaciones de calidad de programas y servicios, integración de expedientes, análisis y seguimiento, hasta su conclusión.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre y edad.	Directa/Presencial.	El nivel de riesgo es bajo. Los datos personales son de categoría estándar, es decir no sensibles.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	Personal a cargo de la práctica de la evaluación, se constituye físicamente en el Inmueble de este Organismo en donde se brinda el programa o servicio y se realizan encuestas a las personas usuarias o beneficiarias obteniendo sus datos personales de los cuales son titulares.	Recabar información para formar un expediente sobre evaluaciones de calidad de programas y servicios, con base a la solicitud de apoyo y dar un seguimiento a la misma hasta su conclusión, de conformidad con el artículo 46 fracción II del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	
Uso	Se revisa y se coteja la información contenida en el expediente de la evaluación, para realizar propuestas sobre el particular.	
Divulgación	**Remisiones:** Se remiten los expedientes de manera íntegra a la Unidad de Transparencia, en atención a solicitudes de información pública y de ejercicio de derechos A.R.C.O. **Transferencias:** No se realizan transferencia de datos personales.	

Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Considerando que no se realizan transferencias de datos personales, no aplica el presente rubro.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Titular(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo	
6.eliminado	
Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Área de Procuración de Fondos
Administrador de Archivos y base de datos	**Nombre**	Arlette Chapoy Gómez
	Cargo	Titular del Área de Procuración de Fondos
	Adscripción	Dirección General del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales		
Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
Arlette Chapoy Gómez. Titular del Área.	Uso, cancelación.	Coteja la documentación de los expedientes para dar validez con su firma.
Rebeca Rojas Ramírez. Supervisor.	Uso, obtención, almacenamiento, divulgación.	Recepción de donativos en especie y económico. Recepción de memorándums, oficios con peticiones/solicitudes de apoyo con entrega de donativos en especie, a personas físicas o morales, integración de expediente y proyectar una resolución.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos		
Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, domicilio, número de teléfono celular y firma.	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Datos Patrimoniales: número de cuenta bancaria y/o CLABE interbancaria de personas físicas y morales privadas,	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	A través de la presentación física o electrónica de documentos con datos personales, realizando donativos en especie y económico o bien realizando peticiones/solicitudes de apoyo con entrega de donativos en especie.	Recabar información para formar un expediente por motivo de la recepción de donativos económicos o en especie, o bien por motivo de peticiones o solicitudes de entrega de apoyo de donativo y dar seguimiento hasta su conclusión, de conformidad con el artículo 37 fracciones I a V del Reglamento Interno de este Organismo.
Almacenamiento	2.eliminado	

Uso	Cotejo de la totalidad de documentos para la autorización sobre el uso de las instalaciones del Organismo y elaboración de contratos correspondiente.
Divulgación	**Remisiones:** Se remiten de forma íntegra a la Unidad de Transparencia por motivo de solicitudes de información o de ejercicio de derechos ARCO, así como para el cotejo de clasificación inicial de información confidencial previo a su publicación en versión pública en el portal de Transparencia. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos. **Transferencias:** No se realizan transferencias.
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Considerando que no se realizan transferencias de datos personales, no aplica el presente rubro.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Jefe(a) de Departamento en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)	
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.	
Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo
6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación
A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD

Nombre del sistema de tratamiento o base de datos		Área de Relaciones Públicas
Administrador de Archivos y base de datos	**Nombre**	Lorena Michele Becerra Álvarez
	Cargo	Titular del Área de Relaciones Públicas
	Adscripción	Dirección General del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	**Tipo de tratamiento que está permitido realizar**	**Obligaciones para el debido tratamiento de los datos personales**
Lorena Michele Becerra Álvarez. Titular del Área.	Uso, obtención, almacenamiento, divulgación, cancelación.	Recepción de memorándums y oficios con peticiones/solicitudes de préstamo y uso de las Instalaciones del Organismo, integración de expediente, y en caso de que proceda, aprobar o validar con su firma mediante la elaboración del contrato de uso.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	**Vía de Obtención**	**Nivel de Riesgo Inherente y Tipo de dato personal**
Datos identificativos: nombre, domicilio, número de teléfono celular y firma.	Directa/Presencial e indirecta/electrónica.	El nivel de riesgo es bajo. Los datos personales son estándar, es decir, no sensibles.
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado	

Tratamiento de datos Personales

Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	A través de la presentación física o electrónica de documentos con datos personales para la elaboración del contrato sobre uso de instalaciones.	Recabar información para formar un expediente con base a una petición y dar seguimiento hasta su conclusión, de conformidad con el artículo 43 fracción VII del Reglamento Interno de este Organismo, artículo 4, 6, 10, 11 y demás relativos y aplicables del Reglamento para el uso, conservación, aprovechamiento y preservación de los auditorios del CAI, explanadas, auditorio CETAM y aulas del Sistema DIF Guadalajara.
Almacenamiento	2.eliminado	
Uso	Cotejo de la totalidad de documentos para la autorización sobre el uso de las instalaciones del Organismo y elaboración de contratos correspondiente.	
Divulgación	**Remisiones:** Se remiten de forma íntegra a la Unidad de Transparencia por motivo de solicitudes de información o de ejercicio de derechos ARCO, así como para el cotejo de clasificación inicial de información confidencial previo a su publicación en versión pública en el portal de Transparencia. Asimismo, se remiten a la Contraloría Interna, para su debida revisión y vigilancia del manejo y aplicación de los recursos públicos. **Transferencias:** No se realizan transferencias.	

Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro y de manera digital, con el programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.
Procedimientos de respaldo de datos personales	Se digitaliza la totalidad de las fojas de cada expediente.
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Considerando que no se realizan transferencias de datos personales, no aplica el presente rubro.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Jefe(a) de Departamento en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha
4.eliminado

Gestión de vulneraciones (Plan de respuesta)
1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo	
6.eliminado	
Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado
Programa General de capacitación	
A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.	
Fecha de actualización del documento de seguridad	18/09/2024

DOCUMENTO DE SEGURIDAD		
Nombre del sistema de tratamiento o base de datos		Unidad de Transparencia
Administrador de Archivos y base de datos	**Nombre**	Miguel Escalante Vázquez
	Cargo	Titular del Área de la Unidad de Transparencia
	Adscripción	Dirección General del Sistema DIF Guadalajara

Las funciones y obligaciones de las personas que traten datos personales

Carácter y nombre de la persona que trata los datos personales	Tipo de tratamiento que está permitido realizar	Obligaciones para el debido tratamiento de los datos personales
Miguel Escalante Vázquez. Titular del Área	Obtención, almacenamiento, uso, divulgación, cancelación.	1.- Recibir solicitudes de manera electrónica, presencial, directa e indirecta, con datos personales identificativos, para el desahogo de una solicitud de información, o solicitud de ejercicio de derechos ARCO, para integrar expediente, analizar la materia de lo solicitado, realizar las remisiones internas, *(en cado de solicitudes ARCO, se remite únicamente el nombre del titular de esos datos personales)*, proyectar y dar respuesta, de Información. 2.- Recepción de escritos de manera electrónica, presencial, directa e indirecta, con datos personales identificativos, derivados de medios de impugnación, y/o requerimiento judicial o administrativo, estudio y análisis de la materia del mismo, para turnar a la unidad administrativa competente, para que realice manifestaciones y el informe de ley el cual es remitido al ITEI. 3.- Al entregar información derivada de medios de impugnación, solicitudes de derechos ARCO, o requerimientos judiciales o administrativos, se realiza la protección de datos personales de terceros. 4.- En las solicitudes de derechos ARCO, la entrega se realiza mediante la acreditación de la identidad del Titular o de su representante. 5.- Recaba datos personales, contenidos en documentos susceptibles de ser publicados y realiza la censura para la protección de datos. Dicha censura también se realiza en documentos que deriven del derecho de acceso a la información.
Yehick Jeanette Flores Padilla. Soporte	Obtención, almacenamiento, uso, divulgación, cancelación.	1.- Recibir solicitudes de manera electrónica, presencial, directa e indirecta, con datos personales identificativos, para el desahogo de una solicitud de información, o solicitud de ejercicio de derechos ARCO, para integrar expediente, analizar la materia de lo solicitado, realizar las remisiones internas, *(en cado de solicitudes ARCO, se remite únicamente el nombre del titular de esos datos personales)*. 2.- Recepción de escritos de manera electrónica, presencial, directa e indirecta, con datos personales identificativos, derivados de medios de impugnación, y/o requerimiento judicial o administrativo, estudio y análisis de la materia del mismo, para turnar a la unidad administrativa competente, para que realice manifestaciones y el informe de ley y ponerlo a consideración del Titular para su remisión al ITEI. 3.- Al entregar información autorizada por el Titular de la Unidad, derivada de medios de impugnación, solicitudes de derechos ARCO, o requerimientos judiciales o administrativos, se realiza la protección de datos personales de terceros. 4.- En las solicitudes de derechos ARCO, la entrega de información autorizada por el Titular del área, se realiza mediante la acreditación de la identidad del Titular o de su representante. 5.- Recaba datos personales, contenidos en documentos susceptibles de ser publicados y realiza la censura para la protección de dato. Dicha censura también se realiza en documentos que deriven del derecho de acceso a la información.

Inventario de Datos Personales que se encuentran dentro de las Bases de Datos

Categoría y listado de Datos Personales	Vía de Obtención	Nivel de Riesgo Inherente y Tipo de dato personal
Datos identificativos: nombre, domicilio, correo electrónico, teléfono particular, teléfono celular, firma, clave única de registro de población (CURP), clave de elector, fotografía y huella digital.	Directa/Presencial (en caso de niñas, niños o adolescentes, los datos personales se obtienen de manera indirecta/presencial por conducto de su representante legal o tutor.	El nivel de riesgo es bajo. Los datos personales son de categoría estándar a excepción de la huella dactilar que es un dato personal sensible.

Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	1.eliminado

Tratamiento de datos Personales		
Procedimiento	**Descripción**	**Finalidad del Tratamiento**
Obtención:	A través de la presentación de solicitudes de información pública, solicitudes de ejercicio de derechos ARCO, recursos de revisión y de transparencia recibidos a través de la Plataforma Nacional de Transparencia, correo electrónico, presencial, y/o por oficio; así como a través de requerimientos judiciales y administrativos.	Desahogar lo relativo al derecho de acceso a la información, así como al ejercicio de derechos ARCO y atender los requerimientos con base a los artículos 19 al 37 del Reglamento de Transparencia y Acceso a la Información Pública del Municipio de Guadalajara.
Almacenamiento	2.eliminado	
Uso	Dependiendo de la naturaleza de la solicitud y/o recurso se turna a la Unidad Administrativa competente para su estudio y desahogo a través de las gestiones de búsqueda, posteriormente notifican a la Unidad de Transparencia el resultado de las gestiones para que esta proyecte respuesta, acuerdo de respuesta o informe de cumplimiento (según corresponda), para luego notificar el resolutivo al requirente de la información o al ITEI adjuntando la atención y documentales aportadas por la Unidad Administrativa.	
Divulgación	**Remisiones:** Se turna a la Unidad Administrativa competente, de conformidad con sus atribuciones y facultades contenidas en el Reglamento Interno del OPD de la Administración Pública Municipal, denominado Sistema Para el Desarrollo Integral de la Familia de Guadalajara, remitiendo únicamente, en el caso de solicitudes de derechos ARCO, el nombre del solicitante y en caso de solicitudes de acceso a información, datos personales identificativos, siempre y cuando sean necesarios para dar atención a la solicitud. **Transferencias:** En caso de incompetencias o competencias parciales, se transfiere la solicitud de información pública, al sujeto obligado del Estado de Jalisco competente, mediante derivación de competencia; asimismo, se transfiere al Instituto de Transparencia, Información Pública y Protección de Datos Personales (ITEI), a fin de rendir informes de ley, en recursos de revisión, en recursos de transparencia y en recursos de protección de datos personales, de conformidad con los artículos 94, 100, 110 y 114 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; artículo 99 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios, artículo 20 del Reglamento de la Ley de Transparencia, y artículo 19 al 37 del Reglamento de Transparencia y Acceso a la Información Pública del Municipio de Guadalajara, por ser necesarias para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales, conforme al aviso de privacidad integral de este Organismo, localizable en el siguiente link: https://difgdl.gob.mx/wp-content/uploads/Aviso-de-Privacidad-Integral-DIF-Guadalajara.pdf	
Bloqueo	Cumplida la finalidad para la cual fueron recabados los datos personales, son bloqueados hasta que se cumple su plazo de conservación señalado en el Catálogo de Disposición Documental; en este lapso, los datos personales no son objeto de tratamiento alguno. Posterior a ello, se procede a su cancelación y destrucción.	
Cancelación/Supresión	La técnica de borrado seguro de datos personales se realiza de manera física, al testar los datos personales de los particulares que no sean titulares de la información solicitada, con lápiz de cera color negro. Respecto a la información digital, se realiza la supresión y cancelación mediante la censura de archivos en formato pdf, a través del programa nitro, o bien con el Sistema Generador de Versiones Públicas 2.0 "Test Data". Una vez cumplido su plazo de conservación señalado en el Catálogo de Disposición Documental, se realiza la propuesta de destrucción a los integrantes del grupo interdisciplinario de archivo y con su aprobación, se lleva a cabo, pues la finalidad es la protección de los datos personales.	
Procedimientos de respaldo de datos personales	Para las solicitudes de acceso a información y los recursos de revisión, de transparencia y de protección de datos personales, se digitaliza la totalidad de las fojas de cada expediente, es decir, los adjuntos de la solicitud, la prevención en los casos en que se haya generado, la respuesta y el resultado de las gestiones aportadas por la(s) Unidad(es), el informe de respuesta, informe de cumplimiento, informes de alcance y actos positivos *(esto último solo en casos de que la respuesta haya sido recurrida con recurso de revisión)*.	
Procedimientos de recuperación de datos personales	En caso de pérdida de datos personales *(por cualquier causa)*, se recurre al respaldo digital para su reposición mediante la impresión, anotando dicha vulneración en la bitácora de vulneraciones.	

Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	Se cuenta con los siguientes controles y mecanismos de seguridad en las transferencias: **Transferencias mediante el traslado de soportes físicos:** a).- El envío se realiza solo a través de personal autorizado y en su caso, con oficio de comisión. b).- Se envía en sobre cerrado y sellado y con la leyenda de protección de información antes señalada. c).- La entrega de la información solo se hace al personal autorizado y facultado por el receptor, recabando el acuse de recibo, con el nombre y firma de quien recibe. d).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencia del área. **Transferencias mediante el traslado físico de soportes electrónicos:** En esta Área, no realiza transferencias físicas en archivos electrónicos con datos personales contenidos en discos flexibles, discos compactos o dispositivos de memoria USB. Sin embargo, en caso de que se llegara a realizar, se utilizarán contraseñas a dichos archivos y se seguirán todas y cada una de las medidas de seguridad aplicadas en el traslado en soportes físicos. **Transferencias mediante el traslado sobre redes electrónicas:** a).- La transmisión de datos personales se realiza en archivos electrónicos mediante la red electrónica, es decir, a través de internet. b).- Se realiza estrictamente hacia correos electrónicos institucionales. c).- La entrega de la información se hace solo al personal autorizado y facultado por el receptor. d).- Se adiciona la leyenda de protección de información confidencial antes señalada. e).- A partir de la aprobación del presente documento, todas las transmisiones, serán registradas en la bitácora de transferencias del área interna.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	**Características del Lugar de Resguardo:** Los datos personales se encuentran resguardados en archiveros con llave, así como en archivos digitales en el disco duro de las computadoras asignadas, mismas que también cuentan con una clave de usuario y contraseña, por lo que solo es posible que acceda el personal que tiene asignado y bajo su resguardo el equipo de cómputo.
Las bitácoras de acceso a los datos personales	1.- Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información: • Nombre y cargo de quien accede; • Identificación del Expediente; • Fojas del Expediente; • Propósito del Acceso; • Fecha y hora de Acceso; • Fecha y hora de Devolución; 2. Las bitácoras se encuentran en soporte físico. 3. Son resguardadas por el(la) Director(a) del área en su oficina que tiene chapa con llave y dentro de archiveros con chapa con llave.
Las bitácoras de vulneraciones a la seguridad de los datos personales	La bitácora de vulneraciones contiene la siguiente información: • Nombre y cargo de quien reporta el incidente; • Fecha y hora en la que ocurrió; • El motivo de la vulneración de seguridad; y, • Las acciones correctivas implementadas de forma inmediata y definitiva.

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

1.- Restauración inmediata de la operatividad mediante respaldos de los soportes electrónicos y versiones digitales de los soportes físicos. 2.- Realizar y presentar la denuncia correspondiente, en caso de que la vulneración fuera resultado de la comisión de un delito. 3.- Llenado del formato "A" por parte de la persona que detectó la vulneración. 4.- Determinación del área, sobre la magnitud de la afectación y elaboración de recomendaciones para los titulares de los datos personales. 5.- Elaboración de informe y propuesta de medidas correctivas a corto y mediano plazo por parte de la Unidad de Transparencia. 6.- Notificación a los titulares de los datos personales, que pudieran resultar afectados en sus derechos patrimoniales o morales, lo cual deberá realizarse en un lapso no mayor a 3 tres días naturales. 7.- Llenado de la bitácora de vulneraciones.

Medidas de seguridad físicas aplicadas a las instalaciones	**Medidas de seguridad administrativas:** Identificación y autentificación de persona autorizada para el tratamiento de datos personales, ya que el personal adscrito porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General; implementación de contraseñas y claves de seguridad en equipos de cómputo; monitoreo y revisión periódica de las medidas; capacitación de personal; se cuenta con equipo interdisciplinario para aprobar baja documental en soportes físicos y electrónicos; firma de carta de confidencialidad para el personal, así como inclusión de cláusulas de confidencialidad en contratos, convenios o instrumentos jurídicos signados con terceros que actúan como encargados en el tratamiento; se cuenta con un manual de procedimientos para el ejercicio de derechos ARCO. **Medidas de seguridad físicas:** Se cuenta con protección de instalaciones, equipos, soportes o bases de datos personales, ya que las 24 horas de todos los días del año hay un elemento de seguridad pública resguardándolas; se utilizan candados o cerraduras en las puertas de acceso a instalaciones y oficinas, así como de archiveros, lo cual impide la libre apertura de puertas, gavetas, cajones y archiveros; se cuenta con sistema de vigilancia en circuito cerrado, se tienen extintores colocados estratégicamente para protección contra incendios; se realiza impermeabilización anual en bóvedas para evitar humedad y deterioro de documentos; se realizan fumigaciones mensuales para evitar deterioro de documentos por plagas y; se cuenta con máquina trituradora de papel. **Medidas de seguridad técnicas:** Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, programas de software; se tiene instalado el firewalls y antivirus en todos los equipos de cómputo; monitorización del uso de datos personales; implementación de técnicas de disociación.
Controles de identificación y autenticación de usuarios	El personal adscrito, porta en todo momento su identificación con el logo Institucional, la cual tiene el nombre, cargo, número de empleado, vigencia y firma de Dirección General. Las computadoras precisan de un nombre de usuario y contraseña para ingresar. A las personas que ingresan a las instalaciones se les solicita se registren en una libreta de control y se les pide su identificación oficial con fotografía, solo cuando es necesario que acrediten su identidad.
Plan de contingencia	5.eliminado

Plan de trabajo

6.eliminado

Mecanismos de monitoreo y revisión de las medidas de seguridad	7.eliminado

Programa General de capacitación

A fin de lograr el debido tratamiento y protección de los datos personales, y para el cumplimiento del principio de responsabilidad, la Unidad de Transparencia, con la coordinación y supervisión del Comité de Transparencia, realizará durante el transcurso del año las siguientes capacitaciones y actualizaciones al personal, conforme al siguiente programa: **Primer trimestre: Principios y deberes establecidos en la Ley de protección de los datos personales en posesión de sujetos obligados**. Objetivo. - Conocer los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, así como los deberes que tienen los sujetos obligados. **Segundo trimestre: Documento de seguridad en materia de protección de Datos personales.** Objetivo. - Obtener recomendaciones en materia de seguridad de datos personales, así como conocer los pasos para implementación de un Sistema de Gestión de Seguridad de Datos Personales y la estructura general del documento de Seguridad. **Tercer trimestre: Aviso de privacidad. Objetivo. -** Identificar los elementos informativos que deberá contener el Aviso de Privacidad en términos de la Ley General de Protección Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los Lineamientos Generales de Protección de Datos Personales para el Sector Público y los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. **Cuarto trimestre: Derechos de acceso, rectificación, cancelación y oposición.** Objetivo. - Conocer los distintos derechos que tienen los titulares de los datos personales, requisitos y procedimiento en el ejercicio de los mismos.

Fecha de actualización del documento de seguridad	18/09/2024

BITACORA DE ACCESO A LOS DATOS PERSONALES					
Nombre y cargo de quien accede	Identificación del Expediente o documento	Fojas del Expediente o documento	Propósito del Acceso	Fecha y hora de Acceso	Fecha y hora de devolución

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)

Nombre y cargo de quien reporta el incidente	Fecha y hora en la que ocurrió	El motivo de la vulneración de seguridad	Las acciones correctivas implementadas de forma inmediata y definitiva

FORMATO A

Vulneraciones a los Sistemas de Información y Bases de Datos

CONTENIDO DE LA BÍTACORA	COMPLETE EL CONTENIDO DE LA BÍTACORA
FECHA DEL INCIDENTE	
NOMBRE	
CARGO	
AREA	
RESPONSABLE DEL ÁREA	
CAUSA DE LA VULNERACIÓN	
SISTEMA(S(DE INFORMACIÓN O BASE(S) DE DATO(S) VULNERAD(O)	
CANTIDAD DE TITULARES	
SOPORTE DE LA INFORMACIÓN VULNERADA	☐ Físico ☐ Electrónico ☐ Mixto
SELECCIONE EL TIPO DE VULNERACIÓN	☐ Pérdida o destrucción no autorizada ☐ Robo, extravío o copia no autorizada ☐ Uso, acceso o tratamiento no autorizado ☐ Daño, alteración o modificación no autorizada
TIPO DE DATOS PERSONALES COMPROMETIDOS	☐ Identificativos ☐ Laborales ☐ Tránsito y Movimientos Migratorios ☐ Académicos ☐ Procedimientos Administrativos o Judiciales ☐ Patrimoniale ☐ Salud ☐ Ideológicos ☐ De origen ☐ Características Personales ☐ Vida Sexual

Nombre y firma de quién reporta	**Nombre y firma del administrador del sistema**	**Nombre y firma del titular del área**

FUNDAMENTO LEGAL

Para estructura y descripción de los sistemas de tratamiento y/o bases de datos personales

1.- Se elimina un párrafo de 09 renglones, que contienen información cuya divulgación pone en riesgo la seguridad del Organismo, la seguridad de los funcionarios públicos, así como la vida, la seguridad y los intereses patrimoniales de los titulares cuyos datos personales se administran en todas las áreas administrativas este Organismo Público Descentralizado. Lo anterior por ser considerado como información reservada de conformidad con el artículo 17.1 fracción I, incisos a) y c) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; acuerdo de la segunda sesión ordinaria del Comité de Transparencia de este Organismo, de fecha 25 de septiembre de 2024 y de conformidad con los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Para: almacenamiento,

2.- Se elimina un párrafo de 04 renglones, que contienen información cuya divulgación pone en riesgo la seguridad del Organismo, la seguridad de los funcionarios públicos, así como la vida, la seguridad y los intereses patrimoniales de los titulares cuyos datos personales se administran en todas las áreas administrativas este Organismo Público Descentralizado. Lo anterior por ser considerado como información reservada de conformidad con el artículo 17.1 fracción I, incisos a) y c) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; acuerdo de la segunda sesión ordinaria del Comité de Transparencia de este Organismo, de fecha 25 de septiembre de 2024 y de conformidad con los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Para los análisis de riesgos

3.- Se elimina un párrafo de 19 renglones, que contienen información cuya divulgación pone en riesgo la seguridad del Organismo, la seguridad de los funcionarios públicos, así como la vida, la seguridad y los intereses patrimoniales de los titulares cuyos datos personales se administran en todas las áreas administrativas este Organismo Público Descentralizado. Lo anterior por ser considerado como información reservada de conformidad con el artículo 17.1 fracción I, incisos a) y c) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; acuerdo de la segunda sesión ordinaria del Comité de Transparencia de este Organismo, de fecha 25 de septiembre de 2024 y de conformidad con los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Para los análisis de brechas

4.- Se elimina un párrafo de 11 renglones, que contienen información cuya divulgación pone en riesgo la seguridad del Organismo, la seguridad de los funcionarios públicos, así como la vida, la seguridad y los intereses patrimoniales de los titulares cuyos datos personales se administran en todas las áreas administrativas este Organismo Público Descentralizado. Lo anterior por ser considerado como información reservada de conformidad con el artículo 17.1 fracción I, incisos a) y c) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; acuerdo de la segunda sesión ordinaria del Comité de Transparencia de este Organismo, de fecha 25 de septiembre de 2024 y de conformidad con los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Para el plan de contingencia

5.- Se elimina un párrafo de 07 renglones, que contienen información cuya divulgación pone en riesgo la seguridad del Organismo, la seguridad de los funcionarios públicos, así como la vida, la seguridad y los intereses patrimoniales de los titulares cuyos datos personales se administran en todas las áreas administrativas este Organismo Público Descentralizado. Lo anterior por ser considerado como información reservada de conformidad con el artículo 17.1 fracción I, incisos a) y c) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; acuerdo de la segunda sesión ordinaria del Comité de Transparencia de este Organismo, de fecha 25 de septiembre de 2024 y de conformidad con los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Para el plan de trabajo

6.- Se elimina un párrafo de 14 renglones, que contienen información cuya divulgación pone en riesgo la seguridad del Organismo, la seguridad de los funcionarios públicos, así como la vida, la seguridad y los intereses patrimoniales de los titulares cuyos datos personales se administran en todas las áreas administrativas este Organismo Público Descentralizado. Lo anterior por ser considerado como información reservada de conformidad con el artículo 17.1 fracción I, incisos a) y c) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; acuerdo de la segunda sesión ordinaria del Comité de Transparencia de este Organismo, de fecha 25 de septiembre de 2024 y de conformidad con los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Para el monitoreo y revisión de las medidas de seguridad

7.- Se elimina un párrafo de 16 renglones, que contienen información cuya divulgación pone en riesgo la seguridad del Organismo, la seguridad de los funcionarios públicos, así como la vida, la seguridad y los intereses patrimoniales de los titulares cuyos datos personales se administran en todas las áreas administrativas este Organismo Público Descentralizado. Lo anterior por ser considerado como información reservada de conformidad con el artículo 17.1 fracción I, incisos a) y c) de la Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios; acuerdo de la segunda sesión ordinaria del Comité de Transparencia de este Organismo, de fecha 25 de septiembre de 2024 y de conformidad con los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.