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		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

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.