

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 brinden 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 (<i>por cualquier causa</i>), 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

e
e
l
s
o
i
o
s
e
r
e
n
s

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 autenticación 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.

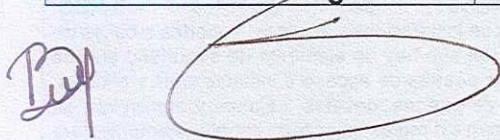
Medidas de seguridad técnicas: Se realizan de copias de seguridad; atención de fallas de equipo electrónico y de cómputo; indicación de software autorizado; realización de labores de mantenimiento, preventivo y correctivo, de equipos electrónicos y de cómputo; se brinda soporte técnico de equipos, sistemas, 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.

[Handwritten signatures and marks at the bottom of the page]

Plan de contingencia	5.eliminado	
Plan de trabajo		
6.eliminado		e o s n e s t a e
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 (LGPDPPO), 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 auditorías 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 instruídas; 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 trámites 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 (<i>por cualquier causa</i>), 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.

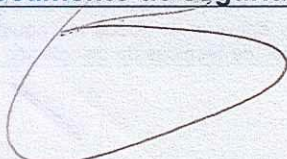
Medidas de seguridad físicas aplicadas a las instalaciones

Medidas de seguridad administrativas: Identificación y autenticación 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 (LGPDPPO), 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 Díaz. 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 (<i>por cualquier causa</i>), 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

n
s
s
o
o
s
e
ir
e
n
s
s

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 autenticación 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.

Rev

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 (<i>por cualquier causa</i>), 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.

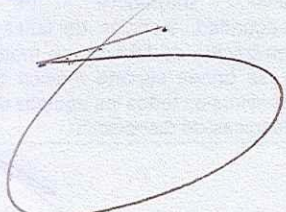
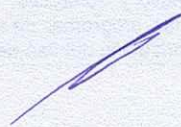
Medidas de seguridad físicas aplicadas a las instalaciones

Medidas de seguridad administrativas: Identificación y autenticación 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 Fariás. Jefe de Turno Xóchitl Araceli Ambríz 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 (<i>por cualquier causa</i>), 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.

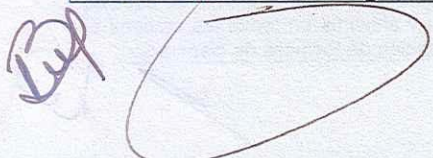
Medidas de seguridad físicas aplicadas a las instalaciones

Medidas de seguridad administrativas: Identificación y autenticación 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 (LGPDPPO), 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.