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

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

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

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

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

Análisis de riesgos

3.eliminado

Análisis de brecha
4.eliminado

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

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

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

Programa General de capacitación

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

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

DOCUMENTO DE SEGURIDAD

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

Las funciones y obligaciones de las personas que traten datos personales

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

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

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

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

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

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

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

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

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

Plan de trabajo

6.eliminado

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

Programa General de capacitación

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

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

DOCUMENTO DE SEGURIDAD

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

Las funciones y obligaciones de las personas que traten datos personales

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

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

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

Tratamiento de datos Personales

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

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

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

Análisis de riesgos

3.eliminado

Análisis de brecha

4.eliminado

Gestión de vulneraciones (Plan de respuesta)

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

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

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

Plan de trabajo

6.eliminado

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

Programa General de capacitación

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

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

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.