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

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

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

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

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

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

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

Análisis de brecha
4.eliminado

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

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

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

Programa General de capacitación

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

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

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.