Órgano Interno de Control

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD		
Nombre del sistema o base de datos		Base de datos personales del Órgano Interno de Control
Respecto del administrador de éste	**Nombre**	Juana Elizabeth Guzmán Elías
	Cargo	Titular del Órgano Interno de Control
	Adscripción	Órgano Interno de Control
Las funciones y obligaciones de las personas que traten datos personales		• **Realizar** el tratamiento conforme a las instrucciones del Responsable de Protección de Datos Personales del Sistema DIF Jalisco; • **Abstenerse** de tratar para finalidades distintas a las instruidas; • **Implementar** las medidas de seguridad conforme a los instrumentos jurídicos aplicables; • **Informar** al Responsable de Protección de Datos Personales del Sistema DIF Jalisco, cuando se tenga conocimiento que ha ocurrido una vulneración; • **Guardar confidencialidad** respecto de los datos personales que recepcione y resguarde por motivo de sus funciones; • **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, y • **Abstenerse de transferir** los datos personales salvo en el caso de que el Responsable de Protección de Datos Personales del Sistema DIF Jalisco, así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.
Inventario de los datos personales		**Datos Personales.** Nombre, edad, sexo, firma, Características físicas, morales, domicilio particular, número de teléfono particular, Clave Única de Registro de Población, Registro Federal de Contribuyentes, los datos de procedimientos juridicos, bienes muebles o inmuebles, fiscales, ingresos.
Niveles de Seguridad de los Datos Personales		**Nivel de Seguridad Básica:** • **Datos de identificación:** Nombre, domicilio, teléfono particular, teléfono celular, correo electrónico, estado civil, firma, firma electrónica, RFC, CURP, cartilla militar, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes y beneficiarios, fotografía, costumbres, idioma o lengua, entre otros. • **Datos laborales**: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.
		Nivel de Seguridad Media: • **Datos patrimoniales:** Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros. • **Datos sobre procedimientos administrativos seguidos en forma de juicio y/o procesos jurisdiccionales:** Información relativa a una persona que se encuentre sujeta como parte o tercero en torno a un procedimiento administrativo seguido en forma de juicio o proceso jurisdiccional en materia laboral, civil, familiar, penal, de justicia para adolescentes, amparo o administrativa, con independencia de su etapa de trámite • **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros. • **Datos de tránsito y movimientos migratorios:** Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.
		Nivel de Seguridad Alta: • **Datos ideológicos:** Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y asociaciones religiosas, entre otros. • **Datos de salud:** Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos y prótesis, entre otros. • **Características biométricas:** Tipo de sangre, ADN, huella dactilar , color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros. • **Vida sexual:** Preferencia sexual, hábitos sexuales, entre otros. • **Origen**: Étnico y racial.

Órgano Interno de Control

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Estructura y descripción de los sistemas de tratamiento y/o bases de datos personales	Se tiene la información resguardada fisicamente en expedientes cerrados, así como en el disco duro de la computadora asignada, a la cual solo tiene acceso el personal responsable del Órgano Interno de Control.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	La información personal que es transferida, se realiza de manera interinstitucional, a los correos electrónicos oficiales asignados al personal de este Organismo, asi como a aquellas autoridades federales y/o estatales y/o municipales, que conforme a sus facultades y atribuciones, resulte legalmente necesario transferirles información personal, agregando en todo caso, una leyenda de Protección de Información Confidencial, en donde se detalla el fin para el cual son transferidos, los datos personales.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	Los datos personales, que se encuentran contenidos en expedientes físicos, se encuentran numerados y resguardados en archiveros, con llave, así como en archivos digitales en el disco duro de la computadora asignada, misma que cuenta con una clave de usuario, a todo lo cual solo tiene acceso el personal responsable del equipo de computo.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	A partir de este momento, se elaboró la bitácora de acceso y operación cotidiana a los datos personales, misma que contiene los siguientes elementos: Nombre del responsable de la información, Nombre de quien accede u opera la información, Motivo de acceso u operación a la Información, Fecha y hora de acceso o de operación del documento, Firma de quien accede u opera la información, Fecha y hora de devolución de la información y Observaciones. De igual forma, se elaboró la bitácora de vulneraciones a la seguridad de los datos personales, la cual contiene los siguientes elementos: Fecha en que ocurrió; Motivo de la vulneración de seguridad; las Acciones correctivas implementadas de forma inmediata y definitiva; El daño, la alteración o modificación no autorizada y Observaciones.

Análisis de riesgos
Considerando que existe el deber de proteger cualquier tipo de dato personal que es tratado en este Organismo, existen riesgos inminentes, que se pudiesen suscitar en cualquier fase del tratamiento de los mismos como seria: la pérdida o destrucción, robo, extravío o expedición de una copia no autorizada, uso, acceso o tratamiento no autorizado, o el daño, alteración o modificación de documentos o expedientes que contengan datos personales, debido a las escasas medidas de seguridad en instalaciones, a la de un mantenimiento eficaz a equipos de computo que almacenan datos personales (medidas de seguridad físicas), a la falta de programas de capacitación y formación del personal en la materia (medidas de seguridad administrativas), a la de falta de contraseñas alfanuméricas seguras para acceder a equipo de computo y de respaldo seguro de información, (medidas de seguridad técnicas).

Análisis de brecha
Los expedientes se encuentran en archiveros deL Órgano Interno de Control, para evitar que el personal no autorizado, tenga acceso a ellos; los archiveros tienen chapa; hay elementos de policía custodiando instalaciones, algunos equipos de computo carecen de contraseñas alfanuméricas de alta seguridad.
Gestión de vulneraciones
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal del organismo que detecte la vulneración deberá proceder al llenado del Formato relativo a la Bitacora de Vulneraciones DIF Jalisco. • Determinación de la magnitud de la afectación y elaboración de recomendaciones para los titulares. • Notificación a titulares en un lapso de 72 horas que de forma significativa vean afectados sus derechos patrimoniales o morales. • En caso de que la vulneración fuera resultado de la comisión de un delito se presentarán las denuncias correspondientes ante las autoridades competentes.

Medidas de seguridad físicas aplicadas a las instalaciones	Se cuenta con oficiales de policía que resguarda las Instalaciones y controla ingresos a las mismas. Para ingresar a las oficinas cuenta con tres puerta metalicas y chapa de seguridad, la cual es cerrada al termino de actividades, restringiendo el ingreso. Además, para ingresar a la oficina de la Contraloria, se cuenta con otra puertas metalicas y con cristal con chapa de seguridad y en el interior de ella se tienen los archiveros en donde se resguardan los expedientes.

Órgano Interno de Control

FICHA DE PROTECCIÓN DE DATOS PERSONALES

DOCUMENTO DE SEGURIDAD	
Controles de identificación y autenticación de usuarios	Los usuarios que tratan información en las oficinas del Órgano Interno de Control son: • Juana Elizabeth Guzmán Elías, Titular del Órgano Interno de Control;
Procedimientos de respaldo y recuperación de datos personales	Se cuenta en expediente físico.
Plan de contingencia	En caso de cualquier vulneración o daño a la seguridad de los datos personales, se deberá actuar con eficiencia, de forma rápida y oportuna, así como en todo momento procurar minimizar el daño, asegurando tener las menores pérdidas posibles y buscando la mayor recuperación de la información en el menor tiempo y costo posible para la dependencia. En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada dirección en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo. El plan de contingencia se encuentra sujeto a modificaciones de conformidad con el plan de trabajo.
Técnicas utilizadas para la supresión y borrado seguro de los datos personales	Por el momento se cuenta con la supresión y borrado de los datos personales de manera manual.

Plan de trabajo
De forma bimestral se verificará por parte del administrador del presente documento de seguridad, que se esté cumpliendo con estas medidas de seguridad y de considerarlo necesario se realizarán propuestas de mejora al Responsable de Protección de Datos Personales del Sistema DIF Jalisco.

Mecanismos de monitoreo y revisión de las medidas de seguridad	Verificación por parte del encargado de Protección de Datos Personales de DIF Jalisco, para constatar que se cumpla con las medidas de seguridad consignadas en el presente documento

Programa General de capacitación		
Temporalidad	**Tipo de capacitación**	**Tipo de personal**
Semestral	• Generalidades de la Ley de Protección de Datos Personales en Posesión de sujetos obligados; • Principios y deberes que deben observarse en el tratamiento de los datos personales; y • Sistema de Gestión, Medidas de seguridad.	Base y Confianza que traten datos