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**	Lic. María de Lourdes Clemente Escencio. Órgano Interno de Control
	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, domicilio particular, número de teléfono particular, correo electrónico particular, Clave Única de Registro de Población.
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	ELIMINADO: Tres renglones, información reservada. Artículo 17.1 fracción I inciso a) LTAIPEJM. Seguridad de los datos personares. Indicaría la condición de los datos y se podría encontrar puntos débiles.
Los controles y mecanismos de seguridad para las transferencias que, en su caso, efectúen	ELIMINADO: Seis renglones, información reservada. Artículo 17.1 fracción I inciso a) LTAIPEJM. Seguridad de los datos personares. Indicaría la condición de los datos y se podría encontrar puntos débiles.
El resguardo de los soportes físicos y/o electrónicos de los datos personales	ELIMINADO: Párrafo, información reservada. Artículo 17.1 fracción I inciso a) LTAIPEJM. Nombre de la bitácora. Medida de Seguridad y Ubicación de Bitácora. Su publicación pondría en riesgo a este Sujeto Obligado, pues indicaría la ubicación de la bitpácora y su posible ateración.
Las bitácoras de acceso, operación cotidiana y vulneraciones a la seguridad de los datos personales	ELIMINADO: Párrafo, información reservada. Artículo 17.1 fracción I inciso a) LTAIPEJM. Nombre de la bitácora. Medida de Seguridad y Ubicación de Bitácora. Su publicación pondría en riesgo a este Sujeto Obligado, pues indicaría la ubicación de la bitpácora y su posible ateración.

Análisis de riesgos
ELIMINADO: Párrafo, información reservada. Artículo 17.1 fracción I inciso a) LTAIPEJM. Seguridad de los datos personares. Indicaría la condición de los datos y se podría encontrar puntos débiles y poner en riesgo los datos personales por la divulgación de los mismos.

Análisis de brecha
ELIMINADO: Párrafo, información reservada. Artículo 17.1 fracción I inciso a) LTAIPEJM. Seguridad de los datos personares. Indicaría la condición de los datos y se podría encontrar puntos débiles y poner en riesgo los datos personales por la divulgación de los mismos.

Gestión de vulneraciones	
• Restauración Inmediata de la operatividad mediante los respaldos de los soportes electrónicos y versiones digitales de los soportes físicos; • El personal encargado 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	ELIMINADO: cinco renglones, Información Reservada, Artículo 17.1 fracción I inciso a) LTAIPEJM medidas de seguridad física. Su publicación pondría en riesgo a este Sujeto Obligado pues reflejaría las posibles vulnerabilidades.
Medidas de seguridad físicas aplicadas a las instalaciones	ELIMINADO: siete renglones, Información Reservada, Artículo 17.1 fracción I inciso a) LTAIPEJM medidas de seguridad física. Su publicación pondría en riesgo a este Sujeto Obligado pues reflejaría las posibles vulnerabilidades.

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: • Lic. María de Lourdes Clemente Escencio. 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 ELIMINADO: Dos rengolones, información reservada Artículo 17.1 Fracción 1 inciso a) LTAIPEJM, seguridad de datos personales. Indicaría la condición de datos y se podría encontrar puntos débiles. 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	Se cuenta con la supresión y borrado de los datos personales con Generación de Versiones Públicas 2.0

Plan de trabajo
De forma anual 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