Documento de seguridad para la Protección de Datos Personales en Posesión del Instituto del Deporte del Estado de Chiapas

El presente documento fue aprobado durante la Primera Sesión Ordinaria del Comité de Transparencia del Instituto del Deporte del Estado de Chiapas, de fecha 21 de Febrero del 2023.

Blvd. Ángel Albino Corzo No. 1600
Tuxtla Gutiérrez, Chiapas; C.P. 29070
Col. Centro
Email: institutodeldeporte1[illegible].com
Tel. (961) 61 3 54 78

Índice

Introducción.

En el Instituto del Deporte del Estado de Chiapas, la información es un activo que debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, administrados y mantenidos por la Entidad. De esta manera, la gestión de la seguridad de la información como parte de un sistema administrativo más amplio, busca establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, aplicando un enfoque basado en los riesgos que la organiza.

En este contexto, el 30 de Agosto de 2017, se publicó la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS) mediante la cual se establecen las bases, principios y procedimientos para garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de sujetos obligados de los tres órdenes de gobierno; se definen las bases mínimas y condiciones homogéneas que regirán el tratamiento de datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (Derechos ARCO) mediante procedimientos sencillos y expeditos; asimismo, se establece la protección de los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de las Dependencias y los Municipios del Estado de Chiapas, con la finalidad de regular su debido tratamiento.

Atendiendo a lo previo y de conformidad con lo establecido en el Artículo 49 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas (LPDPPSOCHIS), se elabora el presente documento de seguridad.

Objetivo.

Describir las medidas de seguridad de Sistema de Gestión de Seguro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia, o disposición de datos personales, así como proteger todos los datos personales sensibles que se recaben y de accesos no autorizados ni tratamientos distintos a los fines para los que fueron recabados mediante cualquiera de los siguientes tipos de soportes:

- Físicos
- Electrónicos

Glosario.

Activo.- todo elemento de valor para el Instituto del Deporte del Estado de Chiapas, involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal que labora en el Instituto, Bienes Muebles, Bienes Inmuebles y Archivo.

Aviso de Privacidad.-Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del objeto del tratamiento de estos.

Bases de datos.-Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Ciclo Vital del Documento.- Las tres fases por las que atraviesan los documentos de archivo, sea cual sea su soporte, desde su recepción o generación de hasta su conservación permanente o baja documental, a saber; archivo de trámite, de concentración o histórico.

Confidencialidad.- es el principio de seguridad de la información que consiste en que la información no pueda estar disponible o divulgarse a personas o procesos no autorizados por cada una de las áreas del Instituto del Deporte del Estado de Chiapas.

Control de Seguridad en la Red.- Configuración de equipo activo de telecomunicaciones y software para proteger la transmisión de datos personales.

Disponibilidad.- es el principio de seguridad de la información que consiste en ser accesible y utilizable a solicitud de las personas o procesos autorizados por el área que corresponda del Instituto del Deporte del Estado de Chiapas.

Documento de Seguridad.- Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por los responsables para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Evaluación de impacto en la protección de datos personales.- Documento mediante el cual las áreas del Instituto del Deporte del Estado de Chiapas que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales sobre determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgo relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normatividad aplicable.

Integridad.- es el principio de la información consistente en garantizar la exactitud y la completitud de la información y los sistemas, de manera que estos no puedan ser modificados sin autorización, ya sea accidental o intencionalmente.

Medidas de seguridad.- Conjunto de acciones, actividades, controles o mecanismos técnicos, administrativos y físicos que permitan proteger los datos personales.

Medidas de seguridad administrativas.- Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional; la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal en materia de datos personales.

Medidas de seguridad físicas.- Conjunto de acciones y mecanismos para proteger el entorno físico de datos personales y de los recursos involucrados en su tratamiento, los cuales pueden ser desde medidas preventivas, cotidianas y correctivas para tener un control de acceso, preservación, conservación de las instalaciones, recursos o bienes en los cuales se resguarda información e incluso a la información misma, asegurando así su disponibilidad e integridad. De manera enunciativa más no limitativa se deben considerar las siguientes actividades:

a) prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b) prevenir el daño o interferencia las instalaciones físicas, áreas críticas de la organización, recursos e información;
c) proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
d) proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas.- Conjunto de acciones y mecanismos para proteger los datos personales que se encuentren en forma digital, así como los sistemas informáticos que les den tratamiento. De manera enunciativa más no limitativa, se deben de considerar las siguientes actividades;

a) Asegurar que el acceso a las bases de datos o a la información, así como los recursos, sea por usuarios identificados y autorizados;

b) Generar un esquema de privilegios para que el usuario realiza las actividades que requiere con motivo de sus funciones;

c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y Hardware, y

d) Gestionar las comunicaciones como operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Red de datos.- Conjunto de componentes electrónicos activos y medios de comunicación conocidos o por conocer tales como fibra óptica, enlaces inalámbricos, cable, entre otros, que permiten el intercambio de paquetes de datos entre dispositivos electrónicos para el procesamiento de información.

Responsables.- Las áreas del Instituto del Deporte del Estado de Chiapas que manejan, resguardan y/o deciden sobre el tratamiento de datos personales.

Seguridad de la información.- La preservación de la confidencialidad como integridad y disponibilidad de la información, que puede abarcar además otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y él no repudio.

Servicios de nube privada.- Modelo de servicio de tecnología de información proporcionada bajo demanda a las áreas universitarias, en infraestructura propiedad de la universidad y que incluye cómputo, almacenamiento, plataforma, seguridad y respaldos.

Servicios de nube pública.- Modelo de servicio de tecnología de información adquirida bajo demanda a terceros, operada en infraestructura ajena al Instituto del Deporte del Estado de Chiapas.

Sistema de gestión de seguridad de datos personales.- Conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y la seguridad de los datos personales.

Sistemas para el tratamiento.- Conjunto de elementos mutuamente relacionados o que interactúan para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos.

Soporte.- Medio, ya sea electrónico o físico, en el que se registra y guarda información, cómo lo es: el papel así como los audiovisuales, fotográficos, fílmicos, digitales, electrónicos, sonoros y visuales, entre otros comas y los que produzca el avance de la tecnología.

Soportes electrónicos.- Son los medios de almacenamiento accesibles solo a través del uso de algún dispositivo electrónico conocido o por conocer, que procese su contenido para examinar, modificar o almacenar los datos; tales como cintas magnéticas de audio, video y datos, fichas microfilm, discos ópticos (CDs, DVDs y blue-rays), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios para el almacenamiento masivo no volátil.

Soportes físicos.- Son los medios de almacenamiento accesibles de forma directa y sin intervención de algún dispositivo para examinar, modificar o almacenar los datos; tales como documentos como oficios, formularios, impresos, escritos autógrafos, documentos de máquina de escribir, fotografías placas radiológicas, carpetas, expedientes, entre otros.

Supresión.- La erradicación del registro de los datos personales conforme a la normativa archivística aplicable, qué resulta en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

Transferencia.- Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Tratamiento.- Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

Vulneración de seguridad.- En cualquier fase del tratamiento de datos, se considera la pérdida o destrucción no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada.

Abreviaturas

Indeporte: Instituto del Deporte del Estado de Chiapas
SGSDP: Sistema de gestión de seguridad de datos personales

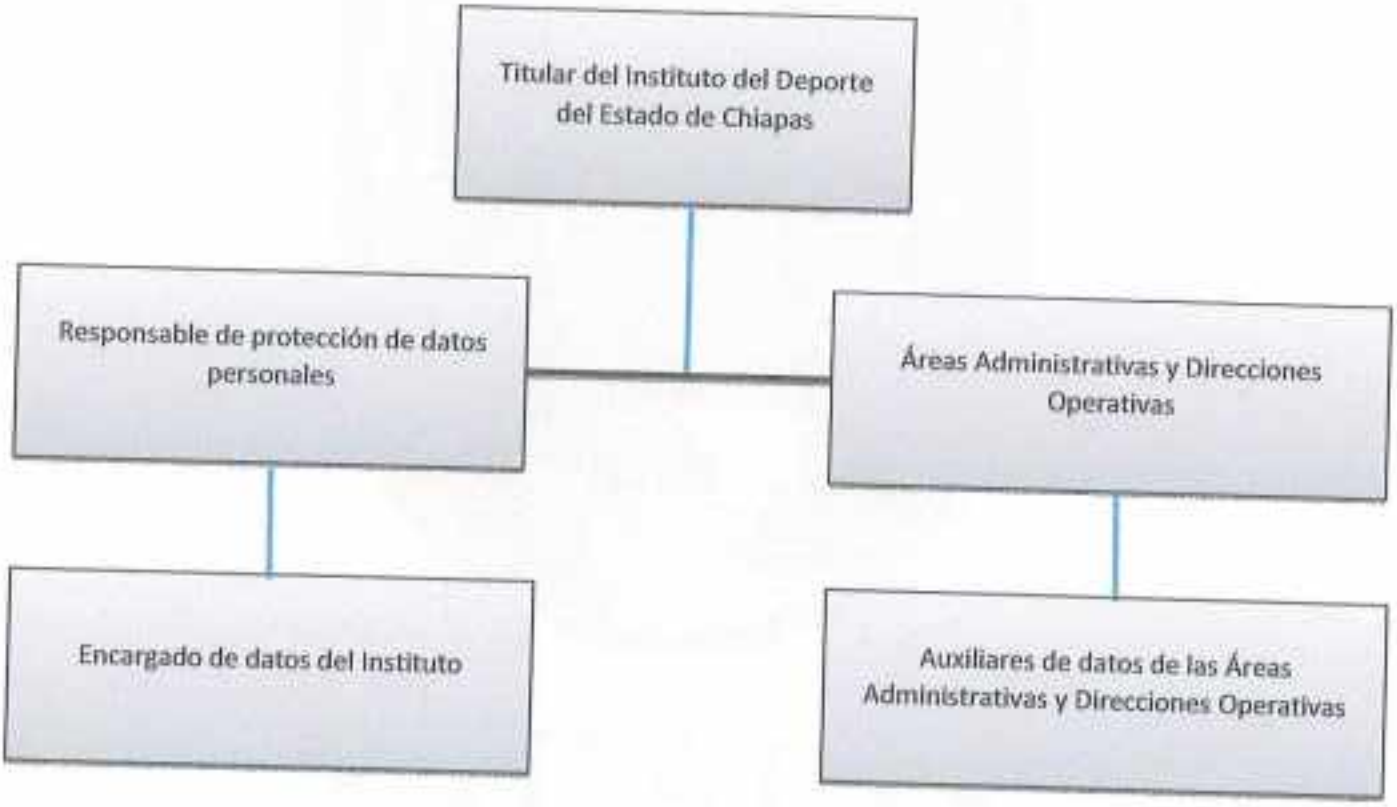
Alcance

Aplica a todas las Áreas Administrativas y Direcciones Operativas que tienen en su poder datos personales y datos personales sensibles.

Funciones y responsabilidades

En el SGSDP del Indeporte, la responsabilidad, autoridad e interrelaciones del personal que trata datos personales, se mantiene con la siguiente cadena de rendición de cuentas:

a) Organigrama del SGSDP



Las funciones y responsabilidades generales de los integrantes del SGSDP son:

Titular

Supervisar que el sistema de gestión de seguridad de datos personales se cumpla de acuerdo a este documento de seguridad.

Responsables

Verificar que el sistema de gestión de seguridad de datos personales se cumplen sus áreas específicas (Administrativas y Direcciones Operativas) de acuerdo a este documento de seguridad.

Encargados:

Mantener el sistema de gestión de seguridad de datos personales en sus áreas específicas (Administrativas y Direcciones Operativas) de acuerdo a este documento de seguridad.

Usuarios:

Utilizar el sistema de gestión de seguridad de datos personales en sus áreas específicas (Administrativas y Direcciones Operativas) de acuerdo a este documento de seguridad.

En la Dirección General del Instituto, los roles son:

Rol	Figura
Titular	Titular
Responsable	Responsable designado por el titular
Encargado	De acuerdo al uso de datos personales definidos en el **anexo 1**: Encargado de Datos
Usuarios	Definido en el **anexo 1** de acuerdo al uso de datos personales

Sistema de gestión de seguridad de datos personales

El Instituto establece y mantiene un sistema de gestión de seguridad de datos personales y documenta sus políticas, sistemas, programas, procedimientos e instrucciones necesarias para asegurar la integridad, confidencialidad y disponibilidad de los datos personales, según la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados en el Estado de Chiapas publicada el 30 de Agosto de 2017, mediante Periódico Oficial Número 315, Decreto Número 239.

Objetivo del SGSDP

El objetivo del SGSDP es: asegurar la integridad, confidencialidad y disponibilidad de la información que contengan datos personales.

El SGSDP cuenta con un inventario con información sobre el tratamiento de datos personales por Área Administrativa o Dirección Operativa responsable, que se encuentra en el **anexo 1** y que considera:

I. El catálogo de recursos a través de los cuales se obtienen los datos personales;
II. Las finalidades de cada tratamiento de datos personales:
III. El catálogo de los tipos de datos personales qué se traten, indicando si son sensibles o no;
IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
V. La lista de funcionarios o empleados universitarios que tienen acceso a los sistemas de tratamiento;
VI. Los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican estás.

En dicho inventario se incluye el ciclo de vida de los datos personales conforme a las siguientes etapas:

- La obtención de los datos personales;
- El almacenamiento de los datos personales;
- El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
- La divulgación de los datos personales considerando las remisiones Y transferencias que, en su caso, se efectúen;
- El bloqueo de los datos personales, en su caso, y
- La cancelación, supresión o destrucción de los datos personales.

Cada sistema de tratamiento sirve para realizar la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, en medios físicos o electrónicos. El detalle de cada sistema de tratamiento de datos personales por Área Administrativa o Dirección Operativa responsable se encuentra en el anexo 1 de este documento.

Análisis de riesgos

El Instituto realiza un análisis de riesgos del tratamiento de los datos personales que se encuentra en el **anexo 2** y de acuerdo a la siguiente metodología:

Los riesgos sobre el tratamiento de datos personales se detectan por Área Administrativa o Dirección Operativa responsable y por cualquier persona que de tratamiento de datos personales.

Se realiza la "matriz de riesgos por tratamiento de datos personales donde se identifica:

Tratamiento de datos personales

Clave de tratamiento de datos personales conforme al inventario

Riesgo probable

Enunciado del riesgo identificado, tomando en cuenta;

- Los requerimientos regulatorios, legales y reglamentarios.
- El valor de los datos personales de acuerdo a si son sensibles.
- No y su ciclo de vida;
- El valor y exposición de los activos involucrados en el tratamiento de los datos personales; Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y los siguientes factores:

- El riesgo inherente a los datos personales tratados;
- La sensibilidad de los datos personales tratados;
- El desarrollo tecnológico;
- Las posibles consecuencias de una vulneración para los titulares;
- Las transferencias de datos personales que se realicen;
- El número de titulares;
- Las móneras iones previas ocurridas en los sistemas de tratamiento, y
- El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Causa probable
La causa probable del riesgo. Pueden usarse las herramientas del análisis de causa raiz como los 5 porqués, diagrama de ishikawa, entre otros.

Probabilidad
La probabilidad subjetiva de que ocurra el riesgo. Es la posibilidad de que ocurra una vulneración de seguridad a los datos personales. Para determinar su probabilidad se toma en cuenta el número de áreas en las que se ha identificado el riesgo. Criterio cuya escala es;

Probabilidad	Escala
De 1 a 3 áreas	bajo
De 4 a 5 áreas	Medio
De 6 a 7 áreas	Alto

Tabla1. Escala de probabilidad

Impacto

El impacto del riesgo se refiere al impacto a las consecuencias negativas, daño o afectación para los titulares que pudieran derivar de una vulneración de seguridad ocurrida en los datos personales. Criterio cuya escala es;

Impacto	Escala
No impacta a la integridad, confidencialidad ni disponibilidad de datos personales	Bajo
No impacta a la integridad, confidencialidad ni disponibilidad de datos personales	Medio
No impacta a la integridad, confidencialidad ni disponibilidad de datos personales	Alto

Cálculo de nivel de valor de riesgo

Para este caso, se asume que el impacto y la probabilidad tienen el mismo valor para la evaluación del riesgo. Se identifica en la gráfica probabilidad versus impacto la zona en la que se encuentra el riesgo identificado para asignarle su nivel de valor de riesgo, que definirá la prioridad con la que se tratarán los riesgos, de la siguiente manera;

Impacto

Alto			
Medio			
Alto			
	Bajo	Medio	Alto

Probabilidad

Nivel de riesgo	Prioridad
Bajo	Planificar acción y documentar en no más de 20 días hábiles desde su detección.
Medio	Planificar acción y documentar en no más de 10 días hábiles desde su detección.
Alto	Planificar acción y documentar inmediatamente.

Una vez identificado los riesgos y su prioridad, se define el tratamiento del riesgo, el cual puede ser;

- **Mitigar:** acciones que minimicen los efectos que pudieran surgir por los riesgos.
- **Eliminar:** acciones que desaparezcan los efectos del riesgo.
- **Transferir:** acciones que trasladen al riesgo. generalmente ocurre cuando no se tiene control total sobre la situación.
- **Aceptar:** generalmente ocurre cuando no se tiene control total sobre la situación.

Una vez identificado el tratamiento de los riesgos se plantean acciones para mitigar, eliminar, transferir o aceptar el riesgo, debiendo considerar los controles de seguridad física, administrativa y técnica para la protección de datos personales.

Cuándo se identifica algún riesgo se debe notificar al responsable de seguridad de datos personales para que lo integre la matriz de riesgos.

Análisis de brecha

El Instituto realiza un análisis de brecha que se encuentra en el **anexo 3** considerando:

- Las medidas de seguridad existentes y efectivas;
- El nivel óptimo de medidas de seguridad y
- Las medidas de seguridad adicionales a las existentes para alcanzar el nivel óptimo.

Plan de trabajo

El Instituto cuenta con un plan de trabajo que define los controles de seguridad a implementar de acuerdo con el resultado de análisis de riesgos y de análisis de brecha, priorizando las medidas de seguridad más relevantes con base en el riesgo detectado.

Lo anterior, considerando los recursos asignados, el personal interno y externo al área, así como las fechas establecidas para la implementación de los controles de seguridad nuevos o faltantes.

Medidas de seguridad para la protección de datos personales

El Instituto implementa medidas de seguridad técnicas, administrativas y físicas para asegurar la protección de los datos personales en el Plan de Trabajo.

Capacitación

Dentro de la capacitación para la comunidad de la DGDU, se estarán estableciendo:

- Charlas informativas sobre temas de protección de datos personales
- Correos masivos con información del tema
- Generación de elementos gráficos con información de protección de datos personales.
- La capacitación debe de incluir las siguientes temas:

  I. Los requerimientos y actualizaciones del sistema de gestión;
  II. La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de estos;
  III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
  IV. Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales Y para la implementación de las medidas de seguridad.

Anexos

Anexos	Descripción
Anexo 1	Inventario
Anexo 2	Análisis de riesgos
Anexo 3	Análisis de brecha

Identificación de los cambios

Fecha de revisión	Versión	Descripción de la modificación	Pagina o sección
08 de Febrero de 2023	1.0	Versión Inicial	

Anexo 1
Inventario de sistemas de tratamiento de datos personales

Identificador único	DDD/DCF-01
Nombre del sistema A1	DDD/DCF
Datos personales (sensibles o no) contenidos en el sistema	CURP, apellido paterno, apellido materno, nombres, fecha de nacimiento, peso, estatura, calle, Colonia, CP, estado civil, celular, tipo de usuario, número de cuenta, plantel, tipo de sangre, alergias, tipo de servicio médico, número de póliza, habitar en caso de emergencia, teléfono en caso de accidente, fecha de registro, edad.
Responsable:	**Dirección de Desarrollo del Deporte**
Nombre:	**Wendy Rubi López Cantoral**
cargo:	**Directora de Desarrollo del Deporte del Instituto del Deporte**
Funciones:	Gestionar el desarrollo del sistema de información segura para proteger la integridad de los datos personales
Obligaciones:	Vigilar el cumplimiento de las acciones que corresponda a cada área.
Encargados:	
Nombre del encargado 1	**Moisés Ramón Hernández Hernández**
Cargo:	**Jefe del Área de Informática**
Funciones:	Desarrollar el Sistema de de Información Para Protección de Datos Personales
Obligaciones :	Mantener actualizados los sistemas operativos del servidor.
Usuarios :	
Nombre del usuario 1	**Wendy Rubi López Cantoral**
cargo:	**Directora de Desarrollo del Deporte**
funciones:	Coordinar el registro de Atletas para las distintas justas deportivas en diversas disciplinas.
Obligaciones :	Realizar los diagnósticos en materia de desarrollo del deporte con los datos obtenidos en las diversas evaluaciones de los atletas.
Nombre del usuario 2	**Mauro Román Chávez Lastra**
Cargo:	**Director de Cultura Física**
Funciones :	Coordinar del registro de participantes en las distintas activaciones físicas y que se desarrollen en el Indeporte.
Obligaciones:	Resguardar los expedientes generados por la participación en las activaciones físicas y cursos de verano que se realicen.

Nombre del sistema A2	**AJ/UT**
Datos personales contenidos en el sistema:	CURP, apellido paterno, apellido materno, nombres, fecha de nacimiento, peso, estatura, calle, Colonia, CP, estado civil, celular, tipo de usuario, número de cuenta, plantel, tipo de sangre, alergias, tipo de servicio médico, número de póliza, habitar en caso de emergencia, teléfono en caso de accidente, fecha de registro, edad.
Responsable:	Dirección de Desarrollo del Deporte
Nombre :	**Wendy Rubi López Cantoral**
Cargo :	**Directora de Desarrollo del Deporte**
funciones:	Proporcionar los datos necesarios a la Unidad de Apoyo Administrativo y al Área Jurídica del padrón de entrenadores en el Instituto del Deporte.
Obligaciones :	Vigilar el cumplimiento de lo establecido en los convenios con los entrenadores del Instituto del Deporte
Encargados:	
Nombre del encargado 1	**Moisés Ramón Hernández Hernández**
Cargo :	**Jefe del Área de Informática**
Funciones :	Desarrollar el Sistema de de Información Para Protección de Datos Personales
Obligaciones :	Mantener actualizados los sistemas operativos del servidor.

Estructura y descripción de los sistemas de tratamiento de datos personales

Direcciones Operativas del Indeporte	
Identificador único	DDD/DCF-01
Nombre del sistema A1	DDD/DCF
Tipo de soporte:	Electrónico e Impreso
Descripción	
Características del lugar donde se resguardan los soportes:	Oficina de las Direcciones de Desarrollo del Deporte y Oficina de la Dirección de Cultura Física

Direcciones Operativas del Indeporte	
Identificador único	AJ/UT
Nombre del sistema A2	AJ/UT
Tipo de soporte:	Electrónico e Impreso
Descripción	
Características del lugar donde se resguardan los soportes:	Oficina de las Direcciones de Desarrollo del Deporte y Oficina de la Dirección de Cultura Física

Anexo 2

Análisis de riesgos

Direcciones Operativas del Indeporte		
Identificador único	DDD/DCF-01	
Nombre del sistema A1	DDD/DCF	
Riesgo	**Impacto**	**Mitigación**
Pérdida, Robo, Daño, Reproducción, Alteración o Uso indebido de la información correspondiente a los datos personales que resguarda el Instituto del Deporte.	Estado de vulneración de los propietarios de los datos personales.	La actualización de las versiones publicas de los informes y documentos establecidos en la página oficial del Instituto, así como la mejora constante del Sistema de Seguridad de Protección de Datos Personales.

Direcciones Operativas del Indeporte		
Identificador único	AJ/UT	
Nombre del sistema A2	AJ/UT	
Riesgo	**Impacto**	**Mitigación**
Pérdida, Robo, Daño, Reproducción, Alteración o Uso indebido de la información correspondiente a los datos personales que resguarda el Instituto del Deporte.	Estado de vulneración de los propietarios de los datos personales.	La actualización de las versiones publicas de los informes y documentos establecidos en la página oficial del Instituto, así como la mejora constante del Sistema de Seguridad de Protección de Datos Personales.

Anexo 3

Análisis de brecha

Direcciones Operativas del Indeporte		
Identificador único	DDD/DCF-01	
Nombre del sistema A1	DDD/DCF	
Medida de seguridad actual	Medida de seguridad Necesaria	Acciones para remediación
Control de acceso fisico no autorizado a los espacios donde se encuentra almacenada la información que contiene datos personales.	Generar la sistematización de la captura, almacenamiento y utilización de los datos personales, con el incremento de medidas de seguridad de carácter informático, tales como son el crear usuarios debidamente autorizados con privilegios especificos para la manipulación de los datos personales en las acciones que competan en sus respectivas direcciones operativas.	Realizar las gestiones administrativas correspondientes para la obtención de la suficiencia presupuestal que permita el desarrollo del proyecto en materia de innovación tecnológica al interior del Instituto del Deporte.

Denominación del área especifica operativa A		
Identificador único	AJ/UT	
Nombre del sistema A2	AJ/UT	
Medida de seguridad	Medida de seguridad necesaria	Acciones para remediación
Control de acceso fisico no autorizado a los espacios donde se encuentra almacenada la información que contiene datos personales.	Generar la sistematización de la captura, almacenamiento y utilización de los datos personales, con el incremento de medidas de seguridad de carácter informático, tales como son el crear usuarios debidamente autorizados con privilegios especificos para la manipulación de los datos personales en las acciones que competan en sus respectivas direcciones operativas.	Realizar las gestiones administrativas correspondientes para la obtención de la suficiencia presupuestal que permita el desarrollo del proyecto en materia de innovación tecnológica al interior del Instituto del Deporte.

Calculo de valor de riesgo en cuanto a impacto y probabilidad de los procesos de cada Área del Instituto del Deporte.

Para la realización del análisis de brecha el responsable deberá considerar lo siguiente:

- **Las medidas de seguridad existente y efectiva;**
- **Las medidas de seguridad faltantes, y**
- **La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.**

PLAN DE TRABAJO

De conformidad con lo dispuesto en el artículo 33, fracción VI, de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nueva o faltante.

Del Programa General de Capacitación

Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos. En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente, el responsable deberá tomar en cuenta lo siguiente:

- Los requerimientos y actualizaciones del sistema de gestión;
- La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;
- Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
- Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Estos serán aprobados por el Comité de Transparencia y será comunicado por la Unidad de Transparencia.

De los Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad

Monitoreo y supervisión periódica de las medidas de seguridad implementadas artículo 63. Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continúa.

Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:

- Los nuevos activos que se incluyan en la gestión de riesgos;
- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras
- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;

- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.

Elaboró

Mtro. Juan Pablo García Mares
Responsable de la Unidad de Transparencia

Aprobó

Ing. Moisés Hernández Hernández
Presidente del Comité de Transparencia