



**Construcción  
de Comunidad**



**Servicios  
Médicos**  
Construcción  
de Comunidad

# Dirección de Servicios Médicos Municipales

## Documento de Seguridad

### Descripción.

El presente instrumento describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Dirección de Servicios Médicos Municipales, como responsable de garantizar la confidencialidad, integridad y disponibilidad de los datos personales que recaba y posee.

### Fecha de actualización

04 de agosto de 2023

*Elaboró*

*Fabiola Marlene Mérida Vélez  
Enlace de Transparencia*

*Validó*

*Dr. Xavier Calderón Alcaraz  
Director de Servicios Médicos Municipales*



**Gobierno de  
Guadalajara**

Mariano Bárcena 997, Alcalde Barranquitas  
Guadalajara, Jalisco, México  
33 1201 7200 y 33 1201 7203  
[serviciosmedicos@guadalajara.gob.mx](mailto:serviciosmedicos@guadalajara.gob.mx)



## Contenido

<b>Introducción</b> .....	3
<b>Marco Normativo</b> .....	4
<b>Glosario</b> .....	5
<b>Sistema de Gestión de Seguridad de los Datos Personales y Sistemas de Tratamiento de Datos Personales por Unidad Administrativa de la Dirección de Servicios Médicos Municipales</b> .....	11
Registro de Asistencia por Biométrico .....	14
Sistema de Videovigilancia .....	27
<b>Análisis de Riesgos</b> .....	41
<b>Análisis de Brecha</b> .....	52
<b>Plan de Contingencia</b> .....	57
<b>Plan de Trabajo del Comité de Transparencia en materia de Protección de Datos Personales e Implementación y Actualización del Documento de Seguridad</b> .....	62
<b>Mecanismos de monitoreo y revisión de medidas de seguridad en las unidades médicas de urgencias y en las áreas administrativas de la Dirección de Servicios Médicos Municipales</b> .....	67
<b>Plan de Capacitación en Materia de Protección de Datos Personales</b> .....	70



## Introducción

El presente instrumento describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Dirección de Servicios Médicos Municipales del Gobierno Municipal de Guadalajara, como responsable de garantizar la confidencialidad, integridad y disponibilidad de los datos personales que recaba y posee.

Este documento, tiene además varias finalidades, la primera de ellas, constituirse como una herramienta de apoyo para las unidades administrativas de la Dirección de Servicios Médicos Municipales, con relación a sus funciones y obligaciones en la protección y confidencialidad de los datos personales que son tratados derivado del cumplimiento de sus propias atribuciones.

La segunda finalidad, es dar certeza a las y los titulares de los datos personales de que esta dependencia en su calidad de responsable, implementa políticas y disposiciones internas para proteger los datos personales y cumple con los principios rectores previstos por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como en los lineamientos emitidos por el Órgano Garante en la materia.

Finalmente, dar cuenta que, las políticas de seguridad plasmadas en el presente documento, pasa por actualizaciones constantes que responden a adecuaciones a sus procesos internos y/o a la implementación o mejora de las medidas de seguridad físicas, técnicas y administrativas, el sistema de gestión de datos personales, el plan de contingencia y/o la modificación de los sistemas de tratamiento.



**Construcción  
de Comunidad**



**Servicios  
Médicos**  
Construcción  
de Comunidad

## Marco Normativo

**Constitución Política de los Estados Unidos Mexicanos**, artículos 6 y 16; última reforma publicada en el Diario Oficial de la Federación el 06 de junio del 2023.

**Constitución Política del Estado de Jalisco**, artículos 4 y 9; última reforma publicada en el periódico Oficial "El Estado de Jalisco" el 16 de marzo de 2023.

**Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados**; publicada en el Diario Oficial de la Federación el 26 de enero del 2017.

**Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios**, publicada en el periódico Oficial "El Estado de Jalisco" el 26 de julio del 2017; última reforma publicada el 15 de mayo del 2021.

**Código de Gobierno Municipal de Guadalajara**, última reforma publicada en la Gaceta Municipal del Gobierno de Guadalajara el 28 de julio de 2023.

**Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas**, del Sistema Nacional de Transparencia Última Reforma DOF 18/11/2022



## Glosario

**Fuente:** Art. 3. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios

**Ajustes Razonables:** Modificaciones y adaptaciones necesarias y adecuadas que no impongan una carga desproporcionada o indebida, cuando se requieran en un caso particular, para garantizar a las personas con discapacidad el goce o ejercicio, en igualdad de condiciones, de los derechos humanos.

**Áreas / Unidades Administrativas:** La Dirección de Servicios Médicos Municipales y las áreas a su cargo en su calidad de responsable que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales.

**Aviso de privacidad:** Documento físico, electrónico o en cualquier formato generado por el del Dirección de Servicios Médicos Municipales, que es puesto a disposición del titular con el objeto de informarle los propósitos principales del tratamiento al que serán sometidos sus datos personales.

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

**Bloqueo:** La identificación y conservación de los datos personales, una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual correspondiente. Durante dicho período los datos personales no podrán ser objeto de tratamiento y concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente o sistema de información que corresponda.

**Comité de Transparencia:** Comité de Transparencia del H. Ayuntamiento Constitucional de Guadalajara en los términos de la Ley de Transparencia, en esta Ley y demás disposiciones aplicables.



**Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos digitales, en recursos compartidos dinámicamente.

**Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular que autoriza el tratamiento de sus datos personales.

**Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

**Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud, información genética, datos biométricos, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

**Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

**Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

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

**Encargado:** Persona física o jurídica, pública o privada, ajena a la Dirección de Servicios Médicos Municipales, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta del responsable.



**Fuentes de acceso público:** Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultados públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a esta Ley y demás disposiciones aplicables;

**ITEI:** Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco;

**INAI:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

**Ley:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Jalisco y sus Municipios;

**Ley de Transparencia:** Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios;

**Ley General:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

**Ley General de Transparencia:** Ley General de Transparencia y Acceso a la Información Pública;

**Medidas compensatorias:** Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios de comunicación masiva u otros de amplio alcance.

**Medidas de seguridad:** conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten garantizar la protección, confidencialidad, disponibilidad e integridad de los datos personales en la Dirección de Servicios Médicos Municipales.

**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, formación y capacitación del personal, en materia de protección de datos personales.

**Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se debe considerar las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de cualquiera de las instalaciones de la Dirección de Servicios Médicos Municipales; incluyendo sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la Dirección de Servicios Médicos Municipales, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir de las instalaciones de la organización; y
- d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.

**Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- b) Generar un esquema de privilegios para que el usuario lleve a cabo 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, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.



**PNT:** La Plataforma Nacional a la que hace referencia el artículo 49, de la Ley General de Transparencia;

**Remisión:** toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado de la Dirección de Servicios Médicos Municipales y el H. Ayuntamiento Constitucional de Guadalajara, con independencia de que se realice dentro o fuera del territorio mexicano.

**Respaldos completos:** Se realiza una copia completa del archivo o medio de almacenamiento.

**Respaldos incrementales:** Sólo se realiza copia de la información que ha sido modificada desde el último respaldo.

**Respaldos diferenciales:** Son similares a los respaldos incrementales en cuanto a realizar la copia de los archivos que han sido modificados desde el último respaldo, sin embargo, estos respaldos se caracterizan por ser acumulativos, es decir cuando se actualiza un archivo, se actualiza en todos los respaldos existentes.

**Responsable:** La Dirección de Servicios Médicos Municipales, señalados en el artículo 1, párrafo 5, de la Ley que determinarán los fines, medios y alcance y demás cuestiones relacionadas con un tratamiento de datos personales.

**Sistema Nacional:** El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales al que hace referencia la Ley General de Transparencia.

**Supresión:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por la Dirección de Servicios Médicos Municipales como responsable.

**Titular:** Persona física a quien pertenecen los datos personales.

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



**Construcción  
de Comunidad**



**Servicios  
Médicos**  
Construcción  
de Comunidad

**Tratamiento.** De manera enunciativa más no limitativa cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados 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; y

**Unidad de Transparencia:** Entendida a la Dirección de Transparencia y Buenas Prácticas del Gobierno Municipal de Guadalajara, Instancia que funge como vínculo entre el responsable y el titular, siendo la misma a la que se hace referencia en el artículo 31 de la Ley de Transparencia y en la presente Ley.



## Sistema de Gestión de Seguridad de los Datos Personales y Sistemas de Tratamiento de Datos Personales por Unidad Administrativa de la Dirección de Servicios Médicos Municipales

Los **Sistemas de Tratamiento de Datos Personales** en la Dirección de Servicios Médicos Municipales, se encuentran organizados por Área o Unidad Administrativa responsable del proceso interno en el cual se da el tratamiento de los datos personales; y se encuentran ajustados a lo dispuesto en el artículo 36 de la Ley de Protección de datos personales en posesión de sujetos obligados del Estado de Jalisco, de tal manera que, cada Sistema de Tratamiento de Datos Personales contiene:

- El nombre de los **sistemas de tratamiento o base de datos personales**;
- El **nombre, cargo y adscripción del administrador** de cada sistema de tratamiento y/o base de datos personales;
- Las funciones y obligaciones de las personas que traten datos personales;
- El **inventario de los datos personales** tratados en cada sistema de tratamiento y/o base de datos personales;
- La **estructura y descripción** de los sistemas de tratamiento y/o bases de datos personales, señalando el tipo de soporte y las características del lugar donde se resguardan;
- Los **controles y mecanismos de seguridad** para las transferencias que, en su caso, se efectúen;
- El **resguardo de los soportes físicos y/o electrónicos** de los datos personales;
- Las **bitácoras de acceso, operación cotidiana y vulneraciones** a la seguridad de los datos personales;
- La **gestión de vulneraciones**;



- Las **medidas de seguridad físicas** aplicadas a las instalaciones;
- Los **controles de identificación y autenticación de usuarios**;
- Los procedimientos de **respaldo y recuperación** de datos personales;
- El **plan de contingencia**;
- Las técnicas utilizadas para la **supresión y borrado seguro** de los datos personales.

Es necesario precisar que los numerales I al XVI del artículo 36 de la Ley de Protección de datos personales en posesión de sujetos obligados del Estado de Jalisco y sus Municipios, son de aplicación general para todas las unidades administrativas, mientras que los numerales XVII, XVIII y XIX son ejecutados por el Comité de Transparencia a través de la Unidad de Transparencia.

En cada uno de los **Sistemas de Tratamiento de Datos Personales** que han sido incluidos en este **Documento de Seguridad**, se establecen las **medidas de seguridad de carácter administrativo, físico y técnico** para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, las cuales constituyen el **Sistema de Gestión de Seguridad de los Datos Personales**.

Por lo que ve al **Plan de Contingencia**, en cada uno de los Sistemas de Tratamiento de Datos Personales que se documenta, se incluye la gestión de incidentes es el proceso de planeación, comunicación y capacidad de acción cuando ocurre un incidente de seguridad.

Posteriormente se profundiza en el **análisis de riesgo como herramienta de prevención de amenazas en el tratamiento de los datos personales**, y el **análisis de brecha** consistente en,



**Construcción  
de Comunidad**



**Servicios  
Médicos**  
Construcción  
de Comunidad

identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados.



Catálogo de Sistemas de Tratamiento de Datos Personales	
Nombre del Sistema	Registro de Asistencia por Biométrico
Coordinación General	Coordinación General de Construcción de Comunidad
Dirección	Dirección de Servicios Médicos Municipales
Administrador	
Nombre	Dr. Juan Manuel de la Torre Hernández
Cargo	Director B
Área	Subdirector de Servicios Administrativos
Funciones y Obligaciones	<p>I. Supervisar que los movimientos y reporte de incidencias de personal de la unidad se realicen oportuna y acorde con la normatividad institucional;</p> <p>II. Gestionar y administrar los recursos humanos, financieros y materiales necesarios para el logro de los objetivos de la Dirección de Servicios Médicos Municipales;</p> <p>III. Definir y establecer políticas administrativas que faciliten la administración estratégica de los procesos de trabajo operativo;</p> <p>IV. Vigilar la correcta aplicación de las políticas y lineamientos en el área de personal, así como llevar el monitoreo del sistema de registro de asistencias por parte del personal;</p> <p>V. Implementar registros de asistencia que den certeza al trabajador día a día, de donde el trabajador obtenga una constancia expresa de lo asentado;</p> <p>VI. Llevar control de registro de asistencia se llevará a cabo mediante tarjetas que se registren en el reloj checador, firma de ingreso y egreso de lista, o cualquier otro sistema de control que se ajuste a las características y necesidades del trabajo prestado, siempre y cuando sea autorizado por la Dirección de Recursos Humanos del Ayuntamiento de Guadalajara o la persona que realice las mismas funciones.</p>
Bases de Datos	Expedientes de personal, Listas de Asistencia, Nombramientos de personal, Control de asistencia de





	personal de la Dirección de Servicios Médicos Municipales y las áreas que la integran.
<b>Personal autorizado para tratamiento (1)</b>	
<b>Nombre de la persona</b>	Lic. Daniel Eduardo Iberri Montes
<b>Nombre del puesto</b>	Colaborador Especializado 2C, Encargado del Departamento de Recursos Humanos
<b>Funciones y Obligaciones</b>	<p>I. Establecer iniciativas hacia el personal para favorecer que los trabajadores crezcan y se desarrollen en su máxima potencia en lo personal y lo profesional; así como, realizar las gestiones administrativas según lo establecido por la normatividad vigente;</p> <p>II. Llevar el control del personal de incidencias que se encuentra en todas las unidades médicas;</p> <p>III. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en las unidades médicas/orgánicas;</p> <p>IV. Coordinarse con logística administrativa de las unidades médicas para el desarrollo pleno de las funciones en materia de personal;</p> <p>V. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>VI. Llevar el control y custodiar los expedientes del personal de la Dirección de Servicios Médicos Municipales para el mejor funcionamiento del departamento;</p> <p>VII. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, teniendo en cuenta las normas vigentes establecidas.</p>
<b>Bases de Datos</b>	Expedientes de personal, Listas de Asistencia, Nombramientos de personal, Control de asistencia de personal de la Dirección de Servicios Médicos Municipales y las áreas que la integran.



Personal autorizado para tratamiento (2)	
Nombre de la persona	María Cristina Sosa Mendoza
Nombre del puesto	Colaborador Especializado 2C, Administradora de la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”
Funciones y Obligaciones	I. Llevar el control del personal de incidencias que se encuentra en la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”; II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”; III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones; IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”; V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”.
Bases de Datos	Control de asistencia de personal de la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”.
Personal autorizado para tratamiento (3)	
Nombre de la persona	L.A.E. Víctor Manuel Anguiano Ramos
Nombre del puesto	Jefe de Unidad Departamental B, Administrador de la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”
Funciones y Obligaciones	I. Llevar el control del personal de incidencias que se encuentra en la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”; II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas,



	<p>e implementarlas en la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”;</p> <p>III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”;</p> <p>V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”.</p>
<b>Bases de Datos</b>	Control de asistencia de personal de la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”.
<b>Personal autorizado para tratamiento (4)</b>	
<b>Nombre de la persona</b>	Mtra. Norma Griselda González Sandoval
<b>Nombre del puesto</b>	Colaborador Especializado 2C, Administradora de la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”
<b>Funciones y Obligaciones</b>	<p>I. Llevar el control del personal de incidencias que se encuentra en la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”;</p> <p>II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”;</p> <p>III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”;</p> <p>V. Tramitar, realizar y controlar los pagos al personal de base,</p>



	becario y suplente, de la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”.
<b>Bases de Datos</b>	Control de asistencia de personal de la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”.
<b>Personal autorizado para tratamiento (5)</b>	
<b>Nombre de la persona</b>	Alma Rubí Gabrielli Garces
<b>Nombre del puesto</b>	Jefe de Unidad Departamental C, Administradora de la Unidad Médica de Urgencias “Dr. Ernesto Arias”
<b>Funciones y Obligaciones</b>	I. Llevar el control del personal de incidencias que se encuentra en la Unidad Médica de Urgencias “Dr. Ernesto Arias”; II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en la Unidad Médica de Urgencias “Dr. Ernesto Arias”; III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones; IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. Ernesto Arias”; V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de la Unidad Médica de Urgencias “Ernesto Arias”.
<b>Bases de Datos</b>	Control de asistencia de personal de la Unidad Médica de Urgencias “Dr. Ernesto Arias”.
<b>Personal autorizado para tratamiento (6)</b>	
<b>Nombre de la persona</b>	Lic. Luis Enrique España Escalante
<b>Nombre del puesto</b>	Colaborador Especializado 6A, Administrador de la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”
<b>Funciones y Obligaciones</b>	I. Llevar el control del personal de incidencias que se



	<p>encuentra en la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”;</p> <p>II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”;</p> <p>III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”;</p> <p>V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”.</p>
<b>Bases de Datos</b>	Control de asistencia de personal de la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”.
<b>Personal autorizado para tratamiento (7)</b>	
<b>Nombre de la persona</b>	Lic. Rosa Elvina Covarrubias Flores
<b>Nombre del puesto</b>	Colaborador Especializado 6A, Administradora de la Unidad Médica de Urgencias “Dr. Ignacio Allende”
<b>Funciones y Obligaciones</b>	<p>I. Llevar el control del personal de incidencias que se encuentra en la Unidad Médica de Urgencias “Dr. Ignacio Allende”;</p> <p>II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en la Unidad Médica de Urgencias “Dr. Ignacio Allende”;</p> <p>III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p>



	<p>IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. Ignacio Allende”;</p> <p>V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de la Unidad Médica de Urgencias “Dr. Ignacio Allende”.</p>
<b>Bases de Datos</b>	Control de asistencia de personal de la Unidad Médica de Urgencias “Dr. Ignacio Allende”.
<b>Personal autorizado para tratamiento (8)</b>	
<b>Nombre de la persona</b>	L.A.E Carlos Augusto Sotelo Rodríguez
<b>Nombre del puesto</b>	Colaborador Especializado 6A, Administrador de Unidades Médicas Básicas y Casas de Salud
<b>Funciones y Obligaciones</b>	<p>I. Llevar el control del personal de incidencias que se encuentra en las Unidades Médicas Básicas y Casas de Salud;</p> <p>II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en las Unidades Médicas Básicas y Casas de Salud;</p> <p>III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>IV. Llevar el control y custodiar los expedientes del personal de adscrito a las Unidades Médicas Básicas y Casas de Salud;</p> <p>V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de las Unidades Médicas Básicas y Casas de Salud.</p>
<b>Bases de Datos</b>	Control de asistencia de personal de las Unidades Médicas Básicas y Casas de Salud.
<b>Tipos de datos personales pertenecientes al Sistema de Tratamiento de Datos Personales</b>	
<b>Inventario</b>	Nombre, número de empleado, biométrico (reconocimiento facial).



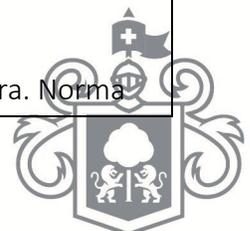
Bases de Datos	Expedientes de personal, Listas de Asistencia, Nombramientos de personal, Control de asistencia de personal de la Dirección de Servicios Médicos Municipales y las áreas que la integran.
No. de Titulares	Entre 501 y 50,000 personas
Controles de seguridad para las bases de datos	Se cierran las oficinas con llave. Los equipos de cómputo cuentan con claves contraseña que únicamente el usuario posee. Se guardan en archivero con las listas de asistencia, controles de asistencia, expedientes de personal. Las instalaciones de la oficina de la cada uno de los Administradores, así como del Jefe del Departamento de Recursos Humanos y la Subdirección de Servicios Administrativos se cierra con llave que únicamente posee el servidor público responsable del Área. Se controla el acceso de personas a las oficinas donde se resguardan los equipos de los Administradores. Las personas servidoras públicas que intervienen en el tratamiento de los datos personales firmaron carta de confidencialidad respecto de los datos personales recabados.
<b>Estructura y descripción del Sistema de Tratamiento de Datos Personales</b>	
Tipo de soporte	Soporte físico y electrónico
Características físicas del lugar de resguardo	Computadora portátil (laptop), archiveros donde se integran los documentos de control de asistencia.
Programas en que se utilizan los D.P.	Correo electrónico, Internet, Hojas de cálculo Excel, PDF.
<b>Resguardo de los soportes físicos y/o electrónicos en que se encuentran los D.P.</b>	
Físicos	I. Mobiliario archiveros. II. <b>Nombre del resguardante del bien mueble:</b> María Cristina Sosa Mendoza/ L.A.E. Victor Anguiano Ramos/ Mtra. Norma Griselda González Sandoval/ Alma Rubí Gabrielli Garces / Lic. Luis Enrique España Escalante/ Lic. Rosa Elvina



	Covarrubias Flores/ L.A.E Carlos Augusto Sotelo Rodríguez.
Electrónicos	<b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\Laptop\ Serie MTM: 20X2S3V600 <b>II. Número Patrimonial:</b> 294424 <b>III. Nombre del resguardante del bien mueble:</b> L.A.E. Victor Anguiano Ramos
	<b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ <b>II. Número Patrimonial:</b> 277371 <b>III. Nombre del resguardante del bien mueble:</b> Lic. Luis Enrique España Escalante
	<b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ <b>II. Número Patrimonial:</b> 277402 <b>III. Nombre del resguardante del bien mueble:</b> Mtra. Norma Griselda González Sandoval
	<b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\Laptop\ Serie MTM: 20X2S3V600 <b>II. Número Patrimonial:</b> 294400 <b>III. Nombre del resguardante del bien mueble:</b> Lic. Rosa Elvina Covarrubias Flores
	<b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ <b>II. Número Patrimonial:</b> F-02780 <b>III. Nombre del resguardante del bien mueble:</b> María Cristina Sosa Mendoza.



	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600</p> <p><b>II. Número Patrimonial:</b> 294420</p> <p><b>III. Nombre del resguardante del bien mueble:</b> Alma Rubí Gabrielli Garces</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\  <b>II. Número Patrimonial:</b> 277227 y 278424  <b>III. Nombre del resguardante del bien mueble:</b> L.A.E Carlos Augusto Sotelo Rodríguez.</p>
<b>Bitácoras de acceso y operación cotidiana</b>	
<b>Bitácoras físicas (ubicación)</b>	N/A
<b>Clave o nombre de la bitácora</b>	N/A
<b>Nombre y cargo del responsable</b>	N/A
<b>Bitácoras electrónicas (ubicación)</b>	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600</p> <p><b>II. Número Patrimonial:</b> 294424</p> <p><b>III. Nombre del resguardante del bien mueble:</b> L.A.E. Victor Anguiano Ramos</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\  <b>II. Número Patrimonial:</b> 277371  <b>III. Nombre del resguardante del bien mueble:</b> Lic. Luis Enrique España Escalante</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\  <b>II. Número Patrimonial:</b> 277402  <b>III. Nombre del resguardante del bien mueble:</b> Mtra. Norma</p>





	Griselda González Sandoval
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600</p> <p><b>II. Número Patrimonial:</b> 294400</p> <p><b>III. Nombre del resguardante del bien mueble:</b> Lic. Rosa Elvina Covarrubias Flores</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600</p> <p><b>II. Número Patrimonial:</b> 294420</p> <p><b>III. Nombre del resguardante del bien mueble:</b> Alma Rubí Gabrielli Garces</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\</p> <p><b>II. Número Patrimonial:</b> F-02780</p> <p><b>III. Nombre del resguardante del bien mueble:</b> María Cristina Sosa Mendoza</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\</p> <p><b>II. Número Patrimonial:</b> 277227 y 278424</p> <p><b>III. Nombre del resguardante del bien mueble:</b> L.A.E Carlos Augusto Sotelo Rodríguez.</p>
Clave o nombre de la bitácora	Bitácora de acceso y operación cotidiana al Registro de Datos Control de Asistencia
Nombre y cargo del responsable	María Cristina Sosa Mendoza/ L.A.E. Víctor Anguiano Ramos/ Mtra. Norma Griselda González Sandoval/ Alma Rubí Gabrielli Garces/ Lic. Luis Enrique España Escalante/ Lic. Rosa Elvina Covarrubias Flores/ L.A.E Carlos Augusto Sotelo Rodríguez.
<b>Bitácoras de vulneraciones de seguridad</b>	
Bitácoras físicas (ubicación)	N/A
Clave o nombre de la bitácora	N/A
Nombre y cargo del	N/A



responsable	
Bitácoras electrónicas (ubicación)	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600</p> <p><b>II. Número Patrimonial:</b> 294424</p> <p><b>III. Nombre del resguardante del bien mueble:</b> L.A.E. Victor Anguiano Ramos</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\  <b>II. Número Patrimonial:</b> 277371  <b>III. Nombre del resguardante del bien mueble:</b> Lic. Luis Enrique España Escalante</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\  <b>II. Número Patrimonial:</b> 277402  <b>III. Nombre del resguardante del bien mueble:</b> Mtra. Norma Griselda González Sandoval</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600  <b>II. Número Patrimonial:</b> 294400  <b>III. Nombre del resguardante del bien mueble:</b> Lic. Rosa Elvina Covarrubias Flores</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600  <b>II. Número Patrimonial:</b> 294420  <b>III. Nombre del resguardante del bien mueble:</b> Alma Rubí Gabrielli Garces</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\  <b>II. Número Patrimonial:</b> F-02780  <b>III. Nombre del resguardante del bien mueble:</b> María Cristina Sosa Mendoza</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\  <b>II. Número Patrimonial:</b> F-02780  <b>III. Nombre del resguardante del bien mueble:</b> María Cristina Sosa Mendoza</p>



	<p>II. <b>Número Patrimonial:</b> 277227 y 278424</p> <p>III. <b>Nombre del resguardante del bien mueble:</b> L.A.E Carlos Augusto Sotelo Rodríguez</p>
<b>Clave o nombre de la bitácora</b>	Bitácora de vulneraciones de seguridad al Registro de Datos Control de Asistencia
<b>Nombre y cargo del responsable</b>	María Cristina Sosa Mendoza/ L.A.E. Victor Anguiano Ramos/ Mtra. Norma Griselda González Sandoval/ Alma Rubí Gabrielli Garces/ Lic. Luis Enrique España Escalante/ Lic. Rosa Elvina Covarrubias Flores/ L.A.E Carlos Augusto Sotelo Rodríguez.

*Fecha de actualización: 04 de agosto de 2023*



Catálogo de Sistemas de Tratamiento de Datos Personales	
Nombre del Sistema	Sistema de Videovigilancia
Coordinación General	Coordinación General de Construcción de Comunidad
Dirección	Dirección de Servicios Médicos Municipales
Administrador	
Nombre	Dr. Juan Manuel de la Torre Hernández
Cargo	Director B
Área	Subdirector de Servicios Administrativos
Funciones y Obligaciones	<p>I. Supervisar que los movimientos y reporte de incidencias de personal de la unidad se realicen oportuna y acorde con la normatividad institucional;</p> <p>II. Gestionar y administrar los recursos humanos, financieros y materiales necesarios para el logro de los objetivos de la Dirección de Servicios Médicos Municipales;</p> <p>III. Definir y establecer políticas administrativas que faciliten la administración estratégica de los procesos de trabajo operativo;</p> <p>IV. Vigilar la correcta aplicación de las políticas y lineamientos en el área de personal, así como llevar el monitoreo del sistema de registro de asistencias por parte del personal;</p> <p>V. Implementar registros de asistencia que den certeza al trabajador día a día, de donde el trabajador obtenga una constancia expresa de lo asentado;</p> <p>VI. Llevar control de registro de asistencia se llevará a cabo mediante tarjetas que se registren en el reloj checador, firma de ingreso y egreso de lista, o cualquier otro sistema de control que se ajuste a las características y necesidades del trabajo prestado, siempre y cuando sea autorizado por la Dirección de Recursos Humanos del Ayuntamiento de Guadalajara o la persona que realice las mismas funciones;</p> <p>VII. Contar con videocámaras, cámaras fijas, cámaras móviles, aéreas y, en general cualquier sistema que permita las</p>



	grabaciones y visualización en espacios con uso público y su posterior tratamiento, a fin de contribuir a la seguridad ciudadana, la prevención de hechos delictivos y la utilización pacífica de las vías y espacios públicos, así como, documentar las faltas administrativas e infracciones relacionadas con el personal.
<b>Bases de Datos</b>	Videovigilancia de la Dirección de Servicios Médicos Municipales y las áreas que la integran.
<b>Personal autorizado para tratamiento (1)</b>	
<b>Nombre de la persona</b>	Lic. Daniel Eduardo Iberri Montes
<b>Nombre del puesto</b>	Colaborador Especializado 2C, Encargado del Departamento de Recursos Humanos
<b>Funciones y Obligaciones</b>	<p>I. Establecer iniciativas hacia el personal para favorecer que los trabajadores crezcan y se desarrollen en su máxima potencia en lo personal y lo profesional; así como, realizar las gestiones administrativas según lo establecido por la normatividad vigente;</p> <p>II. Llevar el control del personal de incidencias que se encuentra en todas las unidades médicas;</p> <p>III. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en las unidades médicas/orgánicas;</p> <p>IV. Coordinarse con logística administrativa de las unidades médicas para el desarrollo pleno de las funciones en materia de personal;</p> <p>V. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>VI. Llevar el control y custodiar los expedientes del personal de la Dirección de Servicios Médicos Municipales para el mejor funcionamiento del departamento;</p> <p>VII. Tramitar, realizar y controlar los pagos al personal de</p>



	base, becario y suplente, teniendo en cuenta las normas vigentes establecidas; VIII. Contar con videocámaras, cámaras fijas, cámaras móviles, aéreas y, en general cualquier sistema que permita las grabaciones y visualización en espacios con uso público y su posterior tratamiento, a fin de contribuir a la seguridad ciudadana, la prevención de hechos delictivos y la utilización pacífica de las vías y espacios públicos, así como, documentar las faltas administrativas e infracciones relacionadas con el personal.
<b>Bases de Datos</b>	Videovigilancia de la Dirección de Servicios Médicos Municipales y las áreas que la integran.
<b>Personal autorizado para tratamiento (2)</b>	
<b>Nombre de la persona</b>	María Cristina Sosa Mendoza
<b>Nombre del puesto</b>	Colaborador Especializado 2C, Administradora de la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”
<b>Funciones y Obligaciones</b>	I. Llevar el control del personal de incidencias que se encuentra en la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”; II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”; III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones; IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”; V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”;



	VI. Contar con videocámaras, cámaras fijas, cámaras móviles, aéreas y, en general cualquier sistema que permita las grabaciones y visualización en espacios con uso público y su posterior tratamiento, a fin de contribuir a la seguridad ciudadana, la prevención de hechos delictivos y la utilización pacífica de las vías y espacios públicos, así como, documentar las faltas administrativas e infracciones relacionadas con el personal.
<b>Bases de Datos</b>	Videovigilancia de la Unidad Médica de Urgencias “Dr. J. Delgadillo Araujo”.
<b>Personal autorizado para tratamiento (3)</b>	
<b>Nombre de la persona</b>	L.A.E. Victor Manuel Anguiano Ramos
<b>Nombre del puesto</b>	Jefe de Unidad Departamental B, Administrador de la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”
<b>Funciones y Obligaciones</b>	<p>I. Llevar el control del personal de incidencias que se encuentra en la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”;</p> <p>II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”;</p> <p>III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”;</p> <p>V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”;</p> <p>VI. Contar con videocámaras, cámaras fijas, cámaras móviles, aéreas y, en general cualquier sistema que permita las</p>



	grabaciones y visualización en espacios con uso público y su posterior tratamiento, a fin de contribuir a la seguridad ciudadana, la prevención de hechos delictivos y la utilización pacífica de las vías y espacios públicos, así como, documentar las faltas administrativas e infracciones relacionadas con el personal.
<b>Bases de Datos</b>	Videovigilancia de la Unidad Médica de Urgencias “Dr. Francisco Ruíz Sánchez”.
<b>Personal autorizado para tratamiento (4)</b>	
<b>Nombre de la persona</b>	Mtra. Norma Griselda González Sandoval
<b>Nombre del puesto</b>	Colaborador Especializado 2C, Administradora de la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”
<b>Funciones y Obligaciones</b>	<p>I. Llevar el control del personal de incidencias que se encuentra en la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”;</p> <p>II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”;</p> <p>III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”;</p> <p>V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”;</p> <p>VI. Contar con videocámaras, cámaras fijas, cámaras móviles, aéreas y, en general cualquier sistema que permita las grabaciones y visualización en espacios con uso público y su posterior tratamiento, a fin de contribuir a la seguridad</p>



	ciudadana, la prevención de hechos delictivos y la utilización pacífica de las vías y espacios públicos, así como, documentar las faltas administrativas e infracciones relacionadas con el personal.
<b>Bases de Datos</b>	Videovigilancia de la Unidad Médica de Urgencias “Dr. Leonardo Oliva Alzaga”.
<b>Personal autorizado para tratamiento (5)</b>	
<b>Nombre de la persona</b>	Alma Rubí Gabrielli Garces
<b>Nombre del puesto</b>	Jefe de Unidad Departamental C, Administradora de la Unidad Médica de Urgencias “Dr. Ernesto Arias”
<b>Funciones y Obligaciones</b>	<p>I. Llevar el control del personal de incidencias que se encuentra en la Unidad Médica de Urgencias “Dr. Ernesto Arias”;</p> <p>II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en la Unidad Médica de Urgencias “Dr. Ernesto Arias”;</p> <p>III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. Ernesto Arias”;</p> <p>V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de la Unidad Médica de Urgencias “Ernesto Arias”;</p> <p>VI. Contar con videocámaras, cámaras fijas, cámaras móviles, aéreas y, en general cualquier sistema que permita las grabaciones y visualización en espacios con uso público y su posterior tratamiento, a fin de contribuir a la seguridad ciudadana, la prevención de hechos delictivos y la utilización pacífica de las vías y espacios públicos, así como, documentar</p>



	las faltas administrativas e infracciones relacionadas con el personal.
<b>Bases de Datos</b>	Videovigilancia de la Unidad Médica de Urgencias “Dr. Ernesto Arias”.
<b>Personal autorizado para tratamiento (6)</b>	
<b>Nombre de la persona</b>	Lic. Luis Enrique España Escalante
<b>Nombre del puesto</b>	Colaborador Especializado 6A, Administrador de la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”
<b>Funciones y Obligaciones</b>	<p>I. Llevar el control del personal de incidencias que se encuentra en la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”;</p> <p>II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”;</p> <p>III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”;</p> <p>V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”;</p> <p>VI. Contar con videocámaras, cámaras fijas, cámaras móviles, aéreas y, en general cualquier sistema que permita las grabaciones y visualización en espacios con uso público y su posterior tratamiento, a fin de contribuir a la seguridad ciudadana, la prevención de hechos delictivos y la utilización pacífica de las vías y espacios públicos, así como, documentar las faltas administrativas e infracciones relacionadas con el personal.</p>



Bases de Datos	Videovigilancia de la Unidad Médica de Urgencias “Dr. Mario Rivas Souza”.
<b>Personal autorizado para tratamiento (7)</b>	
Nombre de la persona	Lic. Rosa Elvina Covarrubias Flores
Nombre del puesto	Colaborador Especializado 6A, Administradora de la Unidad Médica de Urgencias “Dr. Ignacio Allende”
Funciones y Obligaciones	<p>I. Llevar el control del personal de incidencias que se encuentra en la Unidad Médica de Urgencias “Dr. Ignacio Allende”;</p> <p>II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en la Unidad Médica de Urgencias “Dr. Ignacio Allende”;</p> <p>III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>IV. Llevar el control y custodiar los expedientes del personal de adscrito a la Unidad Médica de Urgencias “Dr. Ignacio Allende”;</p> <p>V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de la Unidad Médica de Urgencias “Dr. Ignacio Allende”;</p> <p>VI. Contar con videocámaras, cámaras fijas, cámaras móviles, aéreas y, en general cualquier sistema que permita las grabaciones y visualización en espacios con uso público y su posterior tratamiento, a fin de contribuir a la seguridad ciudadana, la prevención de hechos delictivos y la utilización pacífica de las vías y espacios públicos, así como, documentar las faltas administrativas e infracciones relacionadas con el personal.</p>
Bases de Datos	Videovigilancia de la Unidad Médica de Urgencias “Dr. Ignacio Allende”.



Personal autorizado para tratamiento (8)	
Nombre de la persona	L.A.E Carlos Augusto Sotelo Rodríguez
Nombre del puesto	Colaborador Especializado 6A, Administrador de Unidades Médicas Básicas y Casas de Salud
Funciones y Obligaciones	<p>I. Llevar el control del personal de incidencias que se encuentra en las Unidades Médicas Básicas y Casas de Salud;</p> <p>II. Establecer los mecanismos para el control de asistencia de todo el personal de las áreas médicas y de las administrativas, e implementarlas en las Unidades Médicas Básicas y Casas de Salud;</p> <p>III. Llevar a cabo todos los movimientos del personal y elaborar los registros correspondientes para que no se vean afectados los trabajadores en el ejercicio de sus derechos y obligaciones;</p> <p>IV. Llevar el control y custodiar los expedientes del personal de adscrito a las Unidades Médicas Básicas y Casas de Salud;</p> <p>V. Tramitar, realizar y controlar los pagos al personal de base, becario y suplente, de las Unidades Médicas Básicas y Casas de Salud;</p> <p>VI. Contar con videocámaras, cámaras fijas, cámaras móviles, aéreas y, en general cualquier sistema que permita las grabaciones y visualización en espacios con uso público y su posterior tratamiento, a fin de contribuir a la seguridad ciudadana, la prevención de hechos delictivos y la utilización pacífica de las vías y espacios públicos, así como, documentar las faltas administrativas e infracciones relacionadas con el personal.</p>
Bases de Datos	Videovigilancia de las Unidades Médicas Básicas y Casas de Salud.
Tipos de datos personales pertenecientes al Sistema de Tratamiento de Datos Personales	
Inventario	Imagen, voz de las personas que ingresan y transitan por las instalaciones de la Dirección de Servicios Médicos



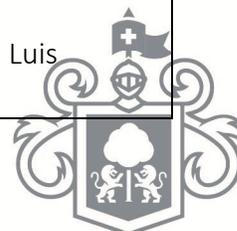
	Municipales.
<b>Bases de Datos</b>	Videovigilancia de la Dirección de Servicios Médicos Municipales y las áreas que la integran.
<b>No. de Titulares</b>	Entre 501 y 50,000 personas
<b>Controles de seguridad para las bases de datos</b>	Se cierran las oficinas con llave. Los equipos de cómputo cuentan con claves contraseña que únicamente el usuario posee. Las instalaciones de la oficina de la cada uno de los Administradores, así como del Jefe del Departamento de Recursos Humanos y la Subdirección de Servicios Administrativos se cierra con llave que únicamente posee el servidor público responsable del Área. Se controla el acceso de personas a las oficinas donde se resguardan los equipos de los Administradores.
<b>Estructura y descripción del Sistema de Tratamiento de Datos Personales</b>	
<b>Tipo de soporte</b>	Soporte electrónico
<b>Características físicas del lugar de resguardo</b>	Computadora portátil (laptop).
<b>Programas en que se utilizan los D.P.</b>	Formato MP4.
<b>Resguardo de los soportes físicos y/o electrónicos en que se encuentran los D.P.</b>	
<b>Físicos</b>	N/A
<b>Electrónicos</b>	<b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600 <b>II. Número Patrimonial:</b> 294424 <b>III. Nombre del resguardante del bien mueble:</b> L.A.E. Victor Anguiano Ramos



	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\  <b>II. Número Patrimonial:</b> 277371  <b>III. Nombre del resguardante del bien mueble:</b> Lic. Luis Enrique España Escalante</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\  <b>II. Número Patrimonial:</b> 277402  <b>III. Nombre del resguardante del bien mueble:</b> Mtra. Norma Griselda González Sandoval</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600  <b>II. Número Patrimonial:</b> 294400  <b>III. Nombre del resguardante del bien mueble:</b> Lic. Rosa Elvina Covarrubias Flores</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\  <b>II. Número Patrimonial:</b> F-02780  <b>III. Nombre del resguardante del bien mueble:</b> María Cristina Sosa Mendoza</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600  <b>II. Número Patrimonial:</b> 294420  <b>III. Nombre del resguardante del bien mueble:</b> Alma Rubí Gabrielli Garces</p>
<b>Bitácoras de acceso y operación cotidiana</b>	
<b>Bitácoras físicas (ubicación)</b>	N/A
<b>Clave o nombre de la</b>	N/A



bitácora	
Nombre y cargo del responsable	N/A
Bitácoras electrónicas (ubicación)	I. <b>Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\Laptop\ Serie MTM: 20X2S3V600 II. <b>Número Patrimonial:</b> 294424 III. <b>Nombre del resguardante del bien mueble:</b> L.A.E. Victor Anguiano Ramos
	I. <b>Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ II. <b>Número Patrimonial:</b> 277371 III. <b>Nombre del resguardante del bien mueble:</b> Lic. Luis Enrique España Escalante
	I. <b>Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ II. <b>Número Patrimonial:</b> 277402 III. <b>Nombre del resguardante del bien mueble:</b> Mtra. Norma Griselda González Sandoval
	I. <b>Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\Laptop\ Serie MTM: 20X2S3V600 II. <b>Número Patrimonial:</b> 294400 III. <b>Nombre del resguardante del bien mueble:</b> Lic. Rosa Elvina Covarrubias Flores
	I. <b>Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\Laptop\ Serie MTM: 20X2S3V600 II. <b>Número Patrimonial:</b> 294420 III. <b>Nombre del resguardante del bien mueble:</b> Alma Rubí Gabrielli Garces
	I. <b>Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ II. <b>Número Patrimonial:</b> F-02780 III. <b>Nombre del resguardante del bien mueble:</b> Lic. Luis Fernando Gómez González





Clave o nombre de la bitácora	Bitácora de acceso y operación cotidiana al Registro de Videovigilancia
Nombre y cargo del responsable	María Cristina Sosa Mendoza/ L.A.E. Victor Anguiano Ramos/ Mtra. Norma Griselda González Sandoval/ Alma Rubí Gabrielli Garces/ Lic. Luis Enrique España Escalante/ Lic. Rosa Elvina Covarrubias Flores/ L.A.E Carlos Augusto Sotelo Rodríguez.
<b>Bitácoras de vulneraciones de seguridad</b>	
Bitácoras físicas (ubicación)	N/A
Clave o nombre de la bitácora	N/A
Nombre y cargo del responsable	N/A
Bitácoras electrónicas (ubicación)	I. <b>Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600 II. <b>Número Patrimonial:</b> 294424 III. <b>Nombre del resguardante del bien mueble:</b> L.A.E. Victor Anguiano Ramos
	I. <b>Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ II. <b>Número Patrimonial:</b> 277371 III. <b>Nombre del resguardante del bien mueble:</b> Lic. Luis Enrique España Escalante
	I. <b>Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ II. <b>Número Patrimonial:</b> 277402 III. <b>Nombre del resguardante del bien mueble:</b> Mtra. Norma Griselda González Sandoval
	I. <b>Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600 II. <b>Número Patrimonial:</b> 294400 III. <b>Nombre del resguardante del bien mueble:</b> Lic. Rosa Elvina Covarrubias Flores



	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Laptop\ Serie MTM: 20X2S3V600</p> <p><b>II. Número Patrimonial:</b> 294420</p> <p><b>III. Nombre del resguardante del bien mueble:</b> Alma Rubí Gabrielli Garces</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Computación\ <b>II. Número Patrimonial:</b> F-02780</p> <p><b>III. Nombre del resguardante del bien mueble:</b> María Cristina Sosa Mendoza</p>
	<p><b>I. Equipo de Cómputo:</b> Equipo de Computación\Equipo de Computación\ Computación\ <b>II. Número Patrimonial:</b> 277227 y 278424</p> <p><b>III. Nombre del resguardante del bien mueble:</b> L.A.E Carlos Augusto Sotelo Rodríguez</p>
<b>Clave o nombre de la bitácora</b>	Bitácora de vulneraciones de seguridad al Registro de Videovigilancia
<b>Nombre y cargo del responsable</b>	María Cristina Sosa Mendoza/ L.A.E. Victor Anguiano Ramos/ Mtra. Norma Griselda González Sandoval/ Alma Rubí Gabrielli Garces/ Lic. Luis Enrique España Escalante/ Lic. Rosa Elvina Covarrubias Flores/ L.A.E Carlos Augusto Sotelo Rodríguez.

*Fecha de actualización: 04 de agosto de 2022*



## Análisis de Riesgos

La seguridad se basa en el entendimiento de la naturaleza del riesgo al que están expuestos los datos personales, el riesgo no se puede erradicar completamente, pero sí se puede minimizar a través de la mejora continua.

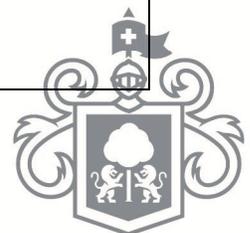
El **objetivo** del **análisis de riesgos** es establecer las características del riesgo que mayor impacto puede tener sobre los datos personales que se tratan en la Dirección de Servicios Médicos Municipales, con el fin de que prioricen y tomen la mejor decisión respecto a los controles más relevantes e inmediatos a implementar.

Las **medidas de seguridad** deberán adoptarse tomando como referencia el nivel de riesgo que presenta cada tratamiento de datos personales; para ello, es necesario calcular los **factores de riesgo** desde el cual se realizan los tratamientos de los datos personales, siendo:

- Factores de riesgo conforme al tipo de dato.



Tipo de datos personales	Descripción	Nivel de Riesgo
Ordinarios	Nombre, Domicilio, Correo electrónico, Teléfono particular, Teléfono celular, RFC, CURP, Clave de elector, Matrícula del servicio militar nacional, Número de pasaporte, Lugar de nacimiento, Fecha de nacimiento, Nacionalidad, Edad, Sexo, Estado civil, Número de seguridad social, Nombramiento, Capacitación, Actividades extracurriculares, Referencias laborales, Solicitud de empleo, Hoja de servicio, Bienes muebles, Bienes inmuebles, Régimen fiscal, Obligaciones fiscales, Declaración fiscal, Historial crediticio, Ingresos, Egresos, Cuentas bancarias, Seguros, Fianzas, Servicios contratados, La correspondiente a una persona relacionada con un procedimiento administrativo, La correspondiente a una persona relacionada con un procedimiento laboral, La correspondiente a una persona relacionada con un	Bajo - Medio





	<p>procedimiento civil, La correspondiente a una persona relacionada con un procedimiento penal, La correspondiente a una persona relacionada con un procedimiento fiscal, La correspondiente a una persona relacionada con un procedimiento familiar, La correspondiente a una persona relacionada con un procedimiento agrario, La correspondiente a una persona relacionada con un procedimiento mercantil, La correspondiente a una persona relacionada con cualquier otra rama del derecho, Trayectoria educativa, Títulos, Cédula profesional, Certificados, Reconocimientos, Solicitud como aspirante, Tránsito y datos migratorios.</p>	
--	---	--

Tipo de datos personales	Descripción	Nivel de Riesgo
<b>Sensibles</b>	Firma, Fotografía, Origen, Etnia, Raza, Color de piel, Color de ojos, Color y tipo de cabello, Estatura, Complexión, Ideología, Creencias, Opinión política, Afiliación política, Opinión pública, Afiliación sindical, Religión, Convicción filosófica, Expediente Clínico, Referencias o descripción de sintomatologías, Enfermedades, Tratamiento de datos genéticos, Incapacidad Médica, Discapacidad, Intervención quirúrgica, Vacunas, Consumo de estupefacientes y/o similares, Uso de aparatos oftalmológicos, Uso de aparatos ortopédicos, Uso de aparatos auditivos, Uso de prótesis, Estado físico, Estado mental, Información sobre la vida sexual, Documentos de Reclutamiento, Documentos de selección, Firma electrónica, Contraseña fiscal, Referencias Personales, Calificaciones, Evaluaciones.	Muy Alto
<b>Biométricos</b>	Huella dactilar, Reconocimiento facial, Reconocimiento de iris, Reconocimiento de retina, Reconocimiento vascular, VOZ	Alto*

\*Alto – muy alto. - atiende a la posibilidad de procesar el dato o automatizarlo.



- Factores de riesgo conforme al tipo de acceso.

Por otra parte, el riesgo por tipo de acceso se mide determinando la cantidad de accesos potenciales a los datos personales que se pretenden proteger por el número de personas que acceden.

Accesibilidad				
Tipos de datos tratados en el sistema de tratamiento	Número de personas que acceden			
	>50	>100	>500	>1000
Datos personales ordinarios	Bajo	Medio	Alto	Muy Alto
Datos personales sensibles	Alto	Alto	Muy alto	Muy alto
Datos personales biométricos	Alto	Muy alto	Muy alto	Muy alto

- Factores de riesgo conforme al tipo de entorno.

Este factor de riesgo relacionado a los entornos mediante a los cuales se accede o hacer uso de los datos personales que se tratan, entre menos control de la accesibilidad ofrezca el entorno, mayor riesgo existe de que se vulnere la seguridad.

Tipo de datos personales	Nivel de Riesgo con controles de accesibilidad básicos	Nivel de Riesgo con controles de accesibilidad estrictos
Acceso entornos de soportes <b>físicos</b>	Medio	Bajo
Acceso entornos de soportes electrónicos o digitales en <b>equipos de computo</b>	Medio	Bajo
Acceso entornos de soportes electrónicos o digitales en <b>servidores locales</b>	Medio	Bajo
Acceso entornos de soportes electrónicos o digitales en <b>nube y servidores remotos</b>	Alto	Medio
Acceso entornos de soportes electrónicos o digitales en <b>plataformas en internet</b>	Alto	Medio

- Factores de riesgo conforme al número de titulares.





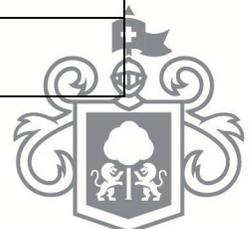
Al riesgo inherente, es necesario sumarle el volumen de titulares, mientras más datos personales diversos se traten puede ser mayor el riesgo de daño en caso de exposición.

Tipo de datos personales	Nivel de Riesgo con controles de accesibilidad básicos
Menos de 100 titulares (>100).	Bajo
Menos de 1000 titulares (>1000).	Medio
Menos de 10,000 (>10,000)	Alto
Más de 10,000 (<10,000).	Muy Alto

- Factores de riesgo conforme al tipo de infraestructura en las instalaciones.

Otro factor de riesgo a valorar es, la calidad de dispositivos de control de incendios, de humedades, mecanismos de ventilación, control de plagas como fauna y flora nociva que pueda dañar los archivos, instalaciones de energía eléctrica adecuadas, ubicación en áreas donde sea poco probable la filtración de líquidos, instalación de puertas abatibles, entre muchos otros, y en general controles relacionados al mantenimiento a instalaciones físicas de la Dirección de Servicios Médicos Municipales donde se localizan áreas de almacenamiento y control de archivos.

Tipo de datos personales	Nivel de Riesgo
Áreas de archivo en instalaciones con medidas de prevención contra incendios, inundaciones, humedad, ventilación, dispositivos de control de descargas de energía eléctrica, fauna y flora nociva, <b>nivel básico.</b>	Muy alto
Áreas de archivo en instalaciones con medidas de prevención contra incendios, inundaciones, humedad, ventilación, dispositivos de control de descargas de energía eléctrica, fauna y flora nociva, <b>nivel medio.</b>	Alto
Áreas de archivo en instalaciones con medidas de prevención contra incendios, inundaciones, humedad,	Medio





ventilación, dispositivos de control de descargas de energía eléctrica, fauna y flora nociva, **nivel alto.**

Al riesgo inherente, es necesario sumarle el volumen de titulares, mientras más datos personales diversos se traten puede ser mayor el riesgo de daño en caso de exposición.

El **riesgo inherente** en los **sistemas de tratamiento de datos personales** puede incrementarse cuando se manejan grandes volúmenes de información personal, como es el caso de la mayoría de los sistemas de tratamiento de la Dirección de Servicios Médicos Municipales, cuando se relacionan distintos tipos de datos o se combinan bases de datos de diferentes fuentes (cruces de información), es necesario estimar la aplicación de **criterios de aceptación de riesgo y de criterios de impacto en el tratamiento de los datos personales**, que deberán ser considerados como directriz para valorar el riesgo, estos son:

- **Criterios de aceptación del riesgo.**

La Dirección de Servicios Médicos Municipales, podría aceptar o no ciertos niveles de riesgo, siempre y cuando la naturaleza del riesgo, sus consecuencias o su probabilidad sean consideradas como muy poco probables o significativas, ponderando que, el manejo masivo de datos personales y los riesgos en su tratamiento, contra los beneficios que conlleva el tratamiento de los datos personales en favor de la población atendida y usuaria de los servicios de salud que ofrece la Dirección de Servicios Médicos Municipales, por ejemplo.

Estos criterios también dependen de las políticas y objetivos de cada sistema de tratamiento de datos personales, considerando que:

1. El **beneficio o el riesgo estimado** en el tratamiento de los datos personales, aplicando diferentes criterios de aceptación correspondientes al riesgo. Por ejemplo, riesgos que pueden resultar del incumplimiento a la Ley que no pueden ser aceptados, por el contrario, cuando el tratamiento de datos traiga consigo la prevención y control de enfermedades urgentes de intervención por el sector salud.



2. Los **criterios de aceptación del riesgo justificado** pueden incluir constancias de consentimiento de los titulares donde se asienten las condiciones que imperan en el tratamiento de los datos personales.

- **Criterios de impacto.**

Consistente en **posible nivel de daño y perjuicio al titular** causado por un **evento negativo** en la seguridad de los datos personales tratados, al evaluar dicho impacto, se deben considerar para cada sistema de tratamiento:

1. El valor de los datos personales tratados para la organización y su importancia de para el sistema de tratamiento aplicable;
2. El incumplimiento en que pudiera incurrir la Dirección de Servicios Médicos Municipales respecto a sus obligaciones legales;
3. Ponderar el beneficio que los de los titulares de datos personales tendrían con el tratamiento de sus datos personales y los posibles daños a la integridad de los titulares de los datos personales ante las posibles vulneraciones que se tienen con cada sistema de tratamiento.

Ahora bien, considerando que **una amenaza tiene el potencial de dañar un activo y de causar una vulneración a la seguridad**, y que estas pueden ser accidentales o deliberadas, provenir de adentro o desde afuera, y afectar a más de un activo al mismo tiempo; estas **vulnerabilidades** son debilidades en la seguridad de los activos y pueden ser identificadas en los siguientes ámbitos:

Ámbito	Principales vulnerabilidades detectadas
Organizacionales	Implementar modificaciones estructurales al organigrama de la Dirección de Servicios Médicos Municipales, implica el traslado de atribuciones y archivos, de un área o unidad administrativa exponiendo los archivos que contienen datos personales entre un área y otra.
De procesos y	<b>1.</b> Procedimientos en los cuales el ciclo de vida de los datos



procedimientos	<p>personales pasa por muchas áreas internas en el Dirección de Servicios Médicos Municipales ampliando la posibilidad que se lleven a cabo incidentes de seguridad.</p> <p>2. Las Políticas Archivísticas del Dirección de Servicios Médicos Municipales se encuentran aún en proceso de elaboración derivado al cumulo de información con que se cuenta y la complejidad en su estructura.</p>
De personal	<p>1. Alta rotación de personal del Dirección de Servicios Médicos Municipales derivado de las necesidades propias del servicio.</p> <p>2. Intervención de personal prestador de servicio social, residentes, internos en áreas médicas.</p> <p>3. Se cuenta con una gran cantidad de recurso humano en el Dirección de Servicios Médicos Municipales, y habiendo una alta rotación de personal, distribuido en varios tipos de jornada de trabajo resulta difícil capacitar en materia de protección de datos personales a la totalidad del personal.</p>

Ámbito	Principales vulnerabilidades detectadas
Del ambiente físico	<p>1. Instalaciones con alto costo de mantenimiento.</p> <p>2. Control de accesos a instalaciones del Dirección de Servicios Médicos Municipales está limitado a las áreas con mayor flujo de personas.</p> <p>3. Presupuesto limitado para la implementación de medidas con altos estándares o de tecnología de punta, que permitan tener la mayor eficiencia en la protección y cuidado de áreas de archivo.</p> <p>4. Poco espacio para el control de archivos de trámite y de concentración.</p>
De la configuración de sistemas de información	<p>1. Acceso a plataformas federales para carga de información de las cuales el Dirección de Servicios Médicos Municipales Jalisco solo es usuario, por lo que se debe contar con bases de datos adicionales.</p>



	<ol style="list-style-type: none"> <li>2. Uso indiscriminado de apps de mensajería por parte del personal del Dirección de Servicios Médicos Municipales.</li> <li>3. Uso de correos electrónicos no oficiales</li> </ol>
Del hardware, software o equipo de comunicación	<ol style="list-style-type: none"> <li>1. Presupuesto limitado para la adquisición de licencias de antivirus y programas de encriptación de información.</li> <li>2. Presupuesto limitado para instalación de cámaras y circuito cerrado en cada inmueble del Dirección de Servicios Médicos Municipales.</li> <li>3. Los equipos de cómputo se pueden volver fácilmente obsoletos ante el rápido avance tecnológico.</li> <li>4. Los softwares se pueden volver fácilmente obsoletos ante el rápido avance tecnológico.</li> <li>5. No se cuenta con suficiente equipo para la digitalización de la totalidad de los expedientes.</li> </ol>
De la relación con terceros.	Los proveedores de servicios tienen alta rotación de personal.

**Identificar escenarios ante vulneración y amenazas.**

Considerando que las **vulnerabilidades no causan daño por sí mismas, ya que se requiere de una amenaza que la explote**; resulta importante identificar las posibles amenazas, para que sea posible monitoreada constantemente, o bien, cuando surja algún cambio hacer las adecuaciones pertinentes.

Ámbito	Principales vulnerabilidades detectadas	Posibles amenazas detectadas
Organizacionales	Implementar modificaciones estructurales al organigrama del Dirección de Servicios Médicos Municipales, implica el traslado de	Falta de controles en entregas de información de un



	atribuciones y archivos, de un área o unidad administrativa exponiendo los archivos que contienen datos personales entre un área y otra.	área a otra.
De procesos y procedimientos	Procedimientos en los cuales el ciclo de vida de los datos personales pasa por muchas áreas internas en el Dirección de Servicios Médicos Municipales ampliando la posibilidad que se lleven a cabo incidentes de seguridad.	Falta de controles en las transferencias de datos personales entre un área a otra.
	Las Políticas Archivísticas del Dirección de Servicios Médicos Municipales se encuentran aún en proceso de elaboración derivado al cumulo de información con que se cuenta y la complejidad en su estructura.	Situaciones que requieren de aplicación normativa interna en materia archivística para determinar responsabilidades.
De personal	Alta rotación de personal del Dirección de Servicios Médicos Municipales derivado de las necesidades propias del servicio.	Fuga de información y/o personal no capacitado
	Intervención de personal prestador de servicio social, residentes, internos en áreas médicas.	Fuga de información
	Se cuenta con una gran cantidad de recurso humano en el Dirección de Servicios Médicos Municipales, y habiendo una alta rotación de personal, distribuido en varios tipos de jornada de trabajo resulta difícil capacitar en materia de protección de datos personales a la totalidad del personal.	Situaciones que requieren de personal capacitado en la materia y que no se tenga en todas las áreas.
Del ambiente físico	Instalaciones con alto costo de mantenimiento.	Contingencias ambientales que ponen en riesgo las infraestructuras como incendios,



		inundaciones, terremotos, entre otros.
	Control de accesos a instalaciones del Dirección de Servicios Médicos Municipales está limitado a las áreas con mayor flujo de personas.	El circuito cerrado no está instalado en la totalidad de inmuebles y las grabaciones se conservan únicamente por un periodo de tiempo corto.
	Presupuesto limitado para la implementación de medidas con altos estándares o de tecnología de punta, que permitan tener la mayor eficiencia en la protección y cuidado de áreas de archivo.	Contingencias ambientales y humanas que ponen en riesgo las infraestructuras.
	Poco espacio para el control de archivos de trámite y de concentración.	Áreas de archivo excedidas en capacidad.

Ámbito	Principales vulnerabilidades detectadas	Posibles amenazas detectadas
De la configuración de sistemas de información	Acceso a plataformas federales para carga de información de las cuales la Dirección de Servicios Médicos Municipales solo es usuario, por lo que se debe contar con bases de datos adicionales.	Afectaciones a las plataformas de donde se extrae información sin posibilidad de corregir vulneraciones al ser solo usuarios de carga y consulta de información no administradores.
	Uso indiscriminado de apps de mensajería por parte del personal de la Dirección de	Fuga de información



	Servicios Médicos Municipales.	
	Uso de correos electrónicos no oficiales	Accesos no autorizados y fuga de información al usar correos electrónicos no oficiales, que utilizan servidores que puedan poner en riesgo la información.
Del hardware, software o equipo de comunicación	Presupuesto limitado para la adquisición de licencias de antivirus y programas de encriptación de información.	Daño de información por software malicioso sin que esta se pueda rescatar
	No se cuenta con suficiente equipo para la digitalización de la totalidad de los expedientes.	Daño, robo, pérdida o destrucción de información contenida en soportes físicos no digitalizados
	Los softwares se pueden volver fácilmente obsoletos ante el rápido avance tecnológico.	Daño, robo, pérdida o destrucción de información contenida en plataformas, bases de datos, sistemas, con software obsoletos que no permitan su tratamiento adecuado
	Los equipos de cómputo se pueden volver fácilmente obsoletos ante el rápido avance tecnológico.	Daño, pérdida o destrucción de información contenida en equipos de cómputo obsoletos que no permitan su tratamiento adecuado
	Presupuesto limitado para instalación de	Daño, robo, pérdida o



	cámaras y circuito cerrado en cada inmueble de la Dirección de Servicios Médicos Municipales.	destrucción de información por accesos no controlados
De la relación con terceros.	Los proveedores de servicios tienen alta rotación de personal.	Daño, robo, pérdida o destrucción de información por accesos no controlados o exceso de encargados en su tratamiento.

Por lo antes expuesto, se concluye que combinación de los **factores de riesgo** que ya han sido analizados, da como **resultado el nivel de riesgo que puede ser latente** según cada tratamiento de datos personales, lo cual contribuye a identificar el nivel de medidas de seguridad que deben implementarse en cada caso.

## Análisis de Brecha



La Dirección de Servicios Médicos Municipales, por la propia naturaleza de sus funciones y atendiendo a las diversas disposiciones legales en materia de protección de datos, realizo un **análisis de brecha** considerando lo expuesto en el **análisis de riesgos** plasmado en el capítulo que antecede.

Aunque se considera que, preferentemente, se debe de plasmar el **nivel de riesgo latente** por cada **sistema de tratamiento de datos personales**, con la finalidad de establecer las estrategias necesarias para identificar los modelos de medidas de seguridad que deben aplicarse a cada uno de ellos, y que como mínimo deben de atender, no obstante, de manera generativa y no limitativa se exponen algunas de las medidas de seguridad sugeridas a ser aplicadas por las áreas o unidades administrativas:

Tipo de medida	Medidas mínimas requeridas para la prevención de los riesgos.
Física	<p>Medida orientada a la <b>protección del entorno físico donde se resguardan los datos personales, tales como instalaciones, áreas de archivo, archiveros, soportes físicos</b>, entre otros, para la prevención de riesgos ya sea por causas humanas provocadas, prevenibles o no prevenibles por llevarse a cabo por caso fortuito o causas de fuerza mayor, se deben considerar, entre otras, las siguientes medidas:</p> <ul style="list-style-type: none"> <li>• Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.</li> <li>• Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.</li> <li>• Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad tales como archiveros con cerradura y llave.</li> <li>• Ingresos a las instalaciones con puertas con cerraduras y llaves, tanto en su exterior como en su interior.</li> <li>• Contar con un plan de verificación de inmuebles y áreas de archivo, para la prevención de riesgos en las instalaciones.</li> <li>• Realizar instalaciones o conexiones hidráulicas o eléctricas que puedan poner en riesgo las áreas donde se resguardan</li> </ul>



	<p>información que contenga datos personales.</p> <ul style="list-style-type: none"> <li>• Uso de candados de seguridad que impidan el traslado de equipo de cómputo de una oficina a otra sin autorización.</li> <li>• Asignar zonas de confidencialidad, donde se resguarden expedientes que contengan información confidencial y con datos sensibles o biométricos, donde se pueda resguardar, custodiar y/o consultar dicha información por personal autorizado.</li> </ul>
--	---

Tipo de medida	Medidas mínimas requeridas para la prevención de los riesgos.
Técnica	<p>Acciones y mecanismos que se valen de la tecnología relacionada con <b>hardware y software</b> para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes medidas:</p> <ul style="list-style-type: none"> <li>• Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados, privilegiando el uso de contraseñas robustas.</li> <li>• Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.</li> <li>• Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.</li> <li>• Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.</li> <li>• Planificar el mantenimiento a los equipos de cómputo, servidores, nubes de almacenamiento de información, depuración de correos electrónicos.</li> <li>• Actualización de software utilizado en las operaciones de las áreas o unidades administrativas, con la intención de que las</li> </ul>



	<p>información siempre se encuentre disponible.</p> <ul style="list-style-type: none"> <li>• Actualización constante de contraseñas de usuarios.</li> <li>• Prevenir el uso de dispositivos móviles de almacenaje como USB, discos externos y similares que puedan dañar los equipos de cómputo por contener software malicioso.</li> <li>• Actualización de antivirus y sistemas de encriptamiento utilizados por la Dirección.</li> <li>• Uso exclusivo de IP autorizadas por la Dirección de Innovación.</li> <li>• Prevenir el borrado, sobre escritura, o destrucción de cualquier información sin autorización del superior jerárquico.</li> <li>• Traslado de equipos de cómputo entre áreas sin que se autorice por el superior jerárquico.</li> <li>• Uso de plataformas e instalación de software, paquetería, apps y similares sin que se autorice por la Dirección de Innovación.</li> <li>• Implementar mecanismos de reportes de fallas de equipos de cómputo, contraseñas, software y sistemas de operación cotidiana utilizados por las áreas o unidades administrativas.</li> <li>• Establecer disposiciones técnicas internas para la programación de respaldos de información periódica que permita el buen mantenimiento de la información.</li> </ul>
--	--

Tipo de medida	Medidas mínimas requeridas para la prevención de los riesgos.
Administrativa	<p>Las <b>medidas de seguridad administrativas</b> serán aquellas las políticas y procedimientos para la gestión, soporte, revisión de la seguridad de la información a nivel organizacional, de identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.</p> <p>De manera enunciativa más no limitativa, se deben considerar las siguientes medidas:</p>



- Contar con políticas de protección de datos personales.
- Documentar los sistemas de tratamiento de datos personales.
- Contar con manuales operativos, organizacionales y/o de procedimientos.
- Contar con Políticas archivistas internas.
- Atender a las capacitaciones en materia de protección de datos personales, transparencia y acceso a la información pública oferte el Comité de Transparencia.
- Uso de declaratorias de confidencialidad tratándose de transferencias de datos personales.
- Implementar las bitácoras de vulneraciones, de acceso y de uso cotidiano (entrada y salida de datos personales).
- Realizar la depuración y respaldo de archivos de forma periódica.
- Designar responsables de los datos personales por área y/o unidad administrativa.



## Plan de Contingencia

*Plan de Contingencia para la atención de incidentes de seguridad, generalidades, tiene como, finalidad, orientar a las unidades administrativas respecto de las medidas que se deben de tomar en el manejo de Incidentes de Seguridad de Datos Personales donde pueda existir riesgos o vulneraciones, y que requieren de una inmediata atención mediante medidas correctivas, a través de los siguientes pasos para la implementación de medidas correctivas de aplicación general, para su implementación se deberán de considerar las particularidades de cada sistema de tratamiento de datos personales de que se trate.*

- **Preparación ante contingencias por incidentes de seguridad de los datos personales.**
  1. **Capacitar al personal** sobre las obligaciones que el área o unidad administrativa de la Dirección de Servicios Médicos Municipales tiene respecto al cumplimiento de las obligaciones en materia de protección de datos personales.
  2. **Sociabilizar con el personal del** área o unidades médicas de urgencias de la Dirección de Servicios Médicos Municipales el **Documento de Seguridad**.
  3. Preparar un portafolio de implementación del **Plan de Contingencia**, que contenga:
    - a) **Documento de Seguridad del Dirección de Servicios Médicos Municipales** que servirá como guía para implementar el **Plan de Contingencia**, según cada sistema de tratamiento;
    - b) Las **Políticas de Protección de Datos Personales** que al efecto emita la **Dirección de Transparencia y Buenas Prácticas del H. Ayuntamiento Constitucional de Guadalajara**;
    - c) **Formatos para implementación** del Documento de Seguridad de la Dirección de Servicios Médicos Municipales;
    - d) **Cámara fotográfica** para recabar evidencia;
    - e) **Directorio** de las personas y/o áreas o unidades médicas de urgencia clave puedan apoyar para la resolución del incidente de seguridad.



- f) Inventario de los sistemas de tratamiento pertenecientes a la Dirección de Servicios Médicos Municipales, Subdirección de Servicios Administrativos y/o Unidades Médicas de Urgencias.
- g) Lista de revisión para dar respuesta a incidentes de seguridad.

- **Procedimientos (pasos a seguir):**

1. **Identificar el Incidente**, para ello se deberá de contar con el *bitácora de identificación del incidente*, que se utilizará para dar seguimiento al incidente, desde el usuario que reporta hasta el área o unidad administrativa que atiende la alerta, además de documentar las alertas que se consideren relevantes o que se relacionen con un incidente de seguridad, en la identificación de un incidente, se sugiere el seguimiento con apoyo de dos personas del área o unidad administrativa, una para evaluar el incidente e identificar activos que pudieran ser afectados, y otra dedicada a documentar y recabar evidencia.

**Para identificar un incidente de seguridad**, se requiere de la detección y/o registro de alertas de seguridad, los cuales son advertencias respecto a cambios en los sistemas de tratamiento, dichas alertas no siempre implican que haya ocurrido un incidente de seguridad. Además, si no se tienen suficientes medidas de seguridad, puede ocurrir un incidente sin que éste se detecte. Se sugiere auxiliarse de la siguiente **lista de alertas de seguridad** sin que sea limitativa, que pueden advertir de una anomalía o cambio no deseado en los activos (archivos físicos o electrónicos que contienen datos personales y forman parte de los sistemas de tratamiento):

Lista de alertas de seguridad	
Entorno (soporte)	Tipo de Alerta
Físico	Alarmas para desastres como incendios o terremotos.
	Alarmas automatizadas contra robos o intrusos en



	instalaciones
	Aviso de desaparición o extravío de equipos de cómputo, medios de almacenamiento o documentos.
	Avisos del personal, clientes, proveedores, autoridades o reportes en medios de comunicación masivos.
	Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento físicos.
<b>Electrónico /Digital</b>	Notificaciones sobre software malicioso o vulnerabilidades técnicas descubiertas, preferentemente de fuentes confiables como agencias nacionales o firmas especializadas en riesgos o seguridad.
	Alertas de sistemas automatizados como firewalls, antivirus, filtros de contenido, sistemas de detección de intrusos (IDS, por sus siglas en inglés) o gestores de seguridad de la información y eventos (SIEM, por sus siglas en inglés).
	Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento automatizados, medios de almacenamiento y equipos de cómputo.

Los incidentes también se podrán **catalogar** por el tipo de evento:

<b>Categorías</b>
<ul style="list-style-type: none"> <li>• Desastre natural (más allá del control humano)</li> </ul>
<ul style="list-style-type: none"> <li>• Inestabilidad social</li> </ul>
<ul style="list-style-type: none"> <li>• Daño físico diverso (accidental o deliberado)</li> </ul>
<ul style="list-style-type: none"> <li>• Falla de infraestructura relacionadas a fallas de energía eléctrica, suministro de agua y drenaje, cableados, aires acondicionados y estructuras del edificio dañadas, entre otros.</li> </ul>
<ul style="list-style-type: none"> <li>• Falla técnica como la saturación de equipos mal funcionamiento de software o fallas de hardware, falta de mantenimiento, entre otros.</li> </ul>
<ul style="list-style-type: none"> <li>• Software malicioso, (malware) como virus, troyanos, software de acceso y control remoto (RAT, por sus siglas en inglés), amenazas persistentes avanzadas</li> </ul>



(APT, por sus siglas en inglés), Ransomware, entre otros.
<ul style="list-style-type: none"> <li>• Ataques técnicos diversos.</li> </ul>
<ul style="list-style-type: none"> <li>• Incumplimiento de reglas o políticas (accidental o deliberado) Uso no autorizado de activos, uso de activos autorizados, pero para finalidades no autorizadas, uso de software, o dispositivos no permitidos, instalación de programas o aplicaciones no autorizadas ilegales, copia o sustracción de documentos o información no autorizada.</li> </ul>
<ul style="list-style-type: none"> <li>• Información dañada, sobre escritura, error de captura o de almacenamiento.</li> </ul>
<ul style="list-style-type: none"> <li>• Intercepción de la información (intervención de comunicaciones, pérdida o extravió de la información)</li> </ul>
<ul style="list-style-type: none"> <li>• Divulgación de contenido perjudicial (contenido ilegal, malicioso, abusivo que pueda dañar derechos morales o patrimoniales de Titulares.</li> </ul>

2. **Investigar el incidente**, se utilizara para documentar el estado del sistema de tratamiento donde ocurrió el incidente, así mismo se deberá de asentar el incidente en la **bitácora de vulneraciones**.
3. **Contener el incidente**, que se utilizará para documentar el aislamiento parcial o total de un sistema, y realizar los respaldos necesarios, si aún se cuenta con ellos, a fin de volver a un estado funcional y puesta en operación en los sistemas de tratamiento en la organización.
4. **Mitigar los efectos del incidente**, que se utilizará para documentar las acciones a corto y mediano plazo después de la contención y el respaldo de la información y minimizar la posibilidad de que éste se vuelva a repetir.
5. **Cierre de investigación**, que se utilizara para dar continuar con la investigación del incidente que dio inició en la fase de contención, de ser necesaria, con él se podrá documentar información para generar evidencia en caso de continuar con un proceso legal ante investigaciones de mayor profundidad en el sistema de tratamiento.



6. **Recuperar la operación del sistema de tratamiento**, en este paso se da seguimiento a las medidas implementadas en la mitigación, y los activos que fueron afectados se reintegran a los sistemas de tratamiento, una vez que se encuentran funcionales o que ya cuentan con medidas de seguridad que los soporten, se sugiere llevar a cabo, monitoreo de los sistemas de tratamiento a fin de identificar si las nuevas medidas de seguridad no causan algún malfuncionamiento en el sistema, o si éstas funcionan adecuadamente; el monitoreo podría ser temporal, o permanente a través del uso de herramientas automatizadas; para documentar si los activos afectados por un incidente regresaron o no a la operación de rutina y si se mitigaron los riesgos que causaron el incidente.



## Plan de Trabajo del Comité de Transparencia en materia de Protección de Datos Personales e Implementación y Actualización del Documento de Seguridad

La implementación del **Plan de Trabajo** en materia de protección de datos personales, que se implemente por año calendario, verá tener como objetivos:

<b>1° Objetivo</b>	Proveer el marco de trabajo necesario para la protección de los datos personales en posesión de la Dirección de Servicios Médicos Municipales.
<b>2° Objetivo</b>	Cumplir con las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales, así como la normatividad que derive de los mismos.
<b>3° Objetivo</b>	Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, a través del Documento de Seguridad y las Políticas de Protección de Datos Personales.
<b>4° Objetivo</b>	Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el Plan de Trabajo se haya implementado de manera integral en la Dirección de Servicios Médicos Municipales, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos en coordinación con la Dirección de Transparencia y Buenas Prácticas.

### Cronograma de trabajo.

El Cronograma de ejecución del Plan de Trabajo será implementado cada año calendario, deberá ser aprobado por el Comité de Transparencia del H. Ayuntamiento Constitucional de Guadalajara, y ejecutado a través de la Dirección de Transparencia y Buenas Prácticas y en Área de Enlace de Transparencia de la Dirección de Servicios Médicos Municipales, las actividades mínimas sugeridas son:



- **Actividades para la actualización del Documento de Seguridad:**

Actividad	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.
Actualizar de Sistemas de Tratamiento de Datos Personales								X	X	X	X	X
Actualizar de inventarios de Datos Personales								X	X	X	X	X

	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.
Actualizar inventario de Plataformas utilizadas por la Dirección de Servicios Médicos Municipales									X	X	X	X
Capacitar para la Actualización de Sistemas de Tratamiento de Datos Personales e Inventarios de Datos Personales									X	X	X	X
Actualizar del Sistema de Gestión de Seguridad de Datos Personales									X	X	X	X
Actualizar de las bitácoras de operación cotidiana									X	X	X	X
Actualizar de las bitácoras de acceso a Datos Personales									X	X	X	X
Capacitar para la Implementación del Sistema de Gestión de Seguridad en los Datos Personales									X	X	X	X
Actualizar el Plan de Contingencia para el manejo de incidentes de seguridad									X	X	X	X
Actualizar las bitácoras de vulneraciones									X	X	X	X
Actualizar formato para identificación de incidentes de seguridad de Datos Personales									X	X	X	X



Actualizar formato para investigación de incidentes de Datos Personales									X	X	X	X
Actualizar formato para contención de incidentes de Datos Personales									X	X	X	X
Actualizar formato para mitigación de incidentes de Datos Personales									X	X	X	X

	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.
Generar formatos para recuperación de incidentes de Datos Personales									X	X	X	X
Generar formatos para mejora continua en la seguridad de los Datos Personales									X	X	X	X
Capacitar: Implementación del Plan de Contingencia para el manejo de incidentes de seguridad									X	X	X	X
Actualizar Documento de Seguridad												X
Remitir Actualizaciones del Documento de Seguridad vía oficio a las áreas responsables de su implementación												X
Presentar el Informe de cumplimiento												X

- Actividades para la actualización del Inventario de programas, sistemas y plataformas informáticas y/o aplicaciones electrónicas o cualquier paquete tecnologías

Actividades	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.
Elaborar inventario de Programas, Sistemas o Plataformas informáticas utilizadas por la Dirección de Servicios Médicos Municipales.												X





Actualizar Sistema de Tratamiento de los Programas, Sistemas o Plataformas informáticas utilizadas por la Dirección de Servicios Médicos Municipales.													X
Generar de Avisos de Privacidad Focalizados.													X

- **Actividades para la actualización de avisos de privacidad.**

Actividad	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.
Actualización del Aviso de Privacidad de la Dirección de Servicios Médicos Municipales				X			X			X		

- **Actividades para supervisar periódicamente el cumplimiento de las obligaciones en materia de Protección de Datos Personales.**

Actividad	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.
Actualizar el Plan de Revisión Periódica de las Medidas de Seguridad de los Datos Personales.	X											
Implementar la evaluación periódica por Unidad Médica de Urgencias de la Dirección de Servicios Médicos Municipales	X											
Implementar la evaluación periódica en la Dirección de Servicios Médicos Municipales	X											
Informe de cumplimiento	X											

- **Actividades para implementación del Programa Anual de Evaluación.**





Actividad	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.
Generar el Plan Anual de Evaluación	X											
Implementar el Plan Anual de Evaluación	X											
Informe de Cumplimiento	X											

El **Plan de Trabajo**, se elabora de conformidad con los siguientes ordenamientos:

- Ley General de Transparencia y Acceso a la Información Pública;
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
- Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios;
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios;
- Lineamientos emitidos por el Sistema Nacional de Transparencia en materia de Datos Personales.



## Mecanismos de monitoreo y revisión de medidas de seguridad en las unidades médicas de urgencias y en las áreas administrativas de la Dirección de Servicios Médicos Municipales

Bajo un esquema de mejora continua, se deberán implementar políticas para evaluar periódicamente el cumplimiento de las obligaciones en Materia de Protección de Datos Personales que la Dirección de Servicios Médicos Municipales, en su calidad de responsable de los datos personales que tratan sus unidades administrativas, para tales efectos se implementarán las siguientes actividades de supervisión y evaluación:

- **Actividades para supervisar periódicamente el cumplimiento de las obligaciones en materia de Protección de Datos Personales.**

Por lo que ve a la **planeación de la supervisión** del cumplimiento de las obligaciones en materia de Protección de Datos Personales, versará sobre las disposiciones legales vigentes en la materia, así como, en las políticas y medidas de seguridad de los datos personales contenidas en el **Documento de Seguridad** y las Políticas de Protección de Datos Personales que emita la Dirección de Transparencia y Buenas Prácticas y que sean implementadas por la Dirección de Servicios Médicos Municipales en las Unidades Médicas de Urgencias y en las áreas administrativas.

La planeación de la supervisión seguirá los siguientes pasos:

Actividad	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.
Actualizar el Plan de supervisión, el cual deberá ser aprobado por el Comité de Transparencia para su implementación.												X
Implementar la supervisión periódica por Unidad Médica de Urgencias de la Dirección de Servicios Médicos Municipales												X
Implementar la supervisión periódica en la Dirección de Servicios Médicos												X





Municipales													
Informe de cumplimiento													X

Para la planeación de la **supervisión**, se deberá contar con reactivos de evaluación a la Dirección de Servicios Médicos Municipales, Unidades Médicas de Urgencias y áreas administrativas, mediante autorización del Comité de Transparencia.

- **Actividades para la evaluación anual del cumplimiento de obligaciones en materia de protección de datos personales.**

La **planeación de actividades de evaluación** del cumplimiento de las obligaciones en materia de Protección de Datos Personales versará sobre las disposiciones legales vigentes en la materia, así como, en las políticas y medidas de seguridad de los datos personales implementadas por la Dirección de Servicios Médicos Municipales a través de su Comité de Transparencia H. Ayuntamiento Constitucional de Guadalajara, las cuales tendrán como objetivo primordial evaluar el cumplimiento de los objetivos y metas trazadas durante el año.

Actividad	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.
Actualizar el Plan Anual de Evaluación, el cual deberá ser aprobado por el Comité de Transparencia para su implementación.												X
Ejecutar el Plan Anual de Evaluación												X
Informe de Cumplimiento												X

La **evaluación** deberá versar sobre las siguientes obligaciones:

- **Implementación del Documento de Seguridad;**
- **Implementación del Sistema de Gestión de Datos Personales;**
- **Implementación del Plan de Contingencia;**
- **Confidencialidad;**
- **Cumplimiento de los Principios rectores de la protección de datos personales;**





## Construcción de Comunidad



**Servicios Médicos**  
Construcción de Comunidad

- Transferencias de Datos Personales;
- Atención de Solicitudes de Ejercicio de Derechos ARCO;
- Cumplimiento de atribuciones del Comité de Transparencia en materia de Protección de Datos Personales;
- Cumplimiento de atribuciones de la Unidad de Transparencia en materia de Protección de Datos Personales;
- Implementación del Plan de Capacitación en materia de Protección de Datos Personales;
- Difusión de la Cultura de la Protección de Datos Personales bajo los lineamientos que al efecto emita la Dirección de Transparencia y Buenas Prácticas.

Lo anterior, considerando que los mecanismos de monitoreo y revisión, aportan elementos para una autoevaluación, y es uno de los mejores puntos de partida para el proceso de planificación y fortalecimiento de la Dirección de Servicios Médicos Municipales perteneciente a la Coordinación General de Construcción de Comunidad, como responsable del cumplimiento de las obligaciones que por disposición legal competen en materia de protección de datos personales, pues permite detectar puntos de oportunidad y mejora, así como para establecer planes a corto, mediano y largo plazo.



## Plan de Capacitación en Materia de Protección de Datos Personales

El **Plan de Capacitación en materia de Protección de Datos Personales**, se ejecutará por conducto de la Dirección de Transparencia y Buenas Prácticas, en coordinación con el área de Enlace de Transparencia de la Dirección de Servicios Médicos Municipales, y se dará cuenta al Comité de Transparencia del avance de cumplimiento de metas, y su **objetivo** primordial es contar con servidoras y servidores públicos conocedores y consientes de sus obligaciones y deberes en materia de protección de datos personales y dotar al personal de habilidades para el tratamiento de los datos personales.

La **planeación de la capacitación** deberá abordar como mínimo las siguientes **temáticas**:

- Conceptos básicos sobre los Datos Personales;
- Ejercicio de Derechos ARCO;
- Obligaciones de los Sujetos Obligados en materia de Protección de Datos Personales;
- Sanciones en materia de incumplimiento a las obligaciones de los Sujetos Obligados en materia de Protección de Datos Personales;
- Implementación del Documento de Seguridad.

El **cronograma de capacitación** deberá ser aprobado por el Comité de Transparencia en la primera sesión ordinaria de cada año calendario, una vez aprobado, de la Dirección de Transparencia y Buenas Prácticas, en coordinación con el área de Enlace de Transparencia de la Dirección de Servicios Médicos Municipales de remitir el Plan de Capacitación a la Coordinación de Capacitación en la que intervendrán el personal de la Dirección de Servicios Médicos Municipales, con la finalidad de acreditar las habilidades formativas del personal.