Jocotepec
Gobierno Municipal

VERSION PUBLICA

DOCUMENTO DE SEGURIDAD DEL MUNICIPIO DE JOCOTEPEC, JALISCO

Introducción

I. Introducción

En la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios se establecen las bases, principios, procedimientos y tratamiento que permite garantizar la protección de datos personales de los ciudadanos en posesión del municipio como sujeto obligado. Teniendo como base dicha normatividad, y de conformidad con sus artículos 3 fracción XIV, artículo 30 al 44 y a la Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales del 2015, emitida por el entonces Instituto Federal de Acceso a la, Información, la cual puede ser consultada en la siguiente liga http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SG SDP(Junio2015).pdf, se crea el presente documento de seguridad. De acuerdo a lo establecido en la Ley en referencia, el Gobierno Municipal de Jocotepec a través de la Unidad de Transparencia, en conjunto con las unidades administrativas, que son las áreas generadoras de información, ha realizado

acciones y actividades que tuvieron como finalidad establecer los cimientos para la creación de este documento. De entre las mismas destaca la elaboración de un listado de datos personales que nos permitió identificar información básica del tratamiento al que son sometidos por cada área del municipio y hacer el primer acercamiento con las áreas sobre la importancia del resguardo de los datos personales. Este documento permitió identificar los trámites municipales y en consecuencia trajo la creación del sistema de tratamiento de datos personales sobre los mismos. Se realizó e implementó a lo largo del 2018 un programa de capacitaciones especializadas en materia de protección de datos personales con la finalidad de concientizar a los servidores públicos sobre el trato lícito y adecuado de los datos personales. Para recabar información precisa y de calidad se realizó un estudio de campo mediante un cuestionario aplicado a través de los enlaces en la materia en cada una de sus áreas, el cual tenía como objetivo detectar medidas de seguridad con las que ya contaba cada área al interior del Municipio y definir posibles riesgos. Una vez contestado el cuestionario, se analizó la información recabada, lo que nos permitió la creación de las medidas de seguridad, tomando como base las necesidades y posibilidades del municipio y las inquietudes y observaciones expresadas por los enlaces de transparencia en sesiones de capacitación. A partir del inventario inicial de datos personales, de las capacitaciones y diversas gestiones con enlaces de transparencia se generaron cada una de las partes que integran el presente documento de seguridad, siguiendo como objetivo el propiciar la protección de los datos personales de la forma más completa y clara posible, ello encaminado a lograr el adecuado tratamiento de los datos personales. El presente documento se guiará por los principios, y conceptos que establece Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.

II. De los sistemas de tratamiento

Se diseñaron los siguientes sistemas de tratamiento:

Trámites municipales			
Datos de identificación			
Fecha de elaboración	Día	Mes	Año
	10	10	2021
Sujeto obligado	Jocotepec, Jalisco		
Unidad administrativa responsable	Todas las áreas que ejecuten trámites. El detalle podrá ser consultado en el inventario de trámites.		
Contenido del Sistema			
Finalidad de sistemas y usos previstos	Obtención de datos de personales derivados del comienzo e integración de cualquier expediente dentro del municipio.		
Las personas o grupos de personas sobre las cuales se obtienen los datos	Ciudadanos que acuden a realizar trámites.		
Procedimiento de recolección	Formatos físicos y electrónicos.*		
Tipo de soporte en donde se contienen los datos personales	Formatos físicos y electrónicos.*		
Características del lugar de resguardo	En las oficinas de las áreas generadoras de la información.		
Estructura básica del sistema y la descripción de los tipos de datos incluidos			
Datos generales del sistema			
Área	Responsable	Cargo	

Municipio de Jocotepec, Jalisco	Responsable de cada área reportado en el inventario de datos personales.	El detalle podrá ser consultado en el inventario de trámites.
Administradores		
Área	Administradores	Cargo
Municipio de Jocotepec, Jalisco	Responsable de cada área reportado en el inventario de datos personales.	El detalle podrá ser consultado en el inventario de trámites.
Datos personales incluidos en el Sistema/Inventario		
Tipo de datos personales		
Nombre, edad, sexo, fecha de nacimiento, lugar de nacimiento, domicilio particular, correo electrónico personal, teléfonos particulares, credencial electoral, documentos oficiales que acrediten su personalidad, número de identificación diversa, estado civil, firma particular, fotografía, CURP, fecha de nacimiento en el RFC, número de cuenta bancaria, parentesco, nombre de familiares, grado académico, huellas digitales, estado de salud.		
Tipo de tratamiento	Tratamiento no automatizado y automatizado. El que requiera el trámite, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.	
Cesión de las que puede ser objeto la información confidencial		

Unidades internas, sujetos obligados, autoridades o terceros a los que en su caso se ceden los datos		
El detalle podrá ser consultado en el inventario de trámites	Seguimiento y conclusión del trámite iniciado por el ciudadano.	
Nivel de protección exigible El detalle podrá ser consultado en el inventario de trámites		Básico
		Medio
	X	Alto
Fundamento legal		
Art. 3, fracción IX de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios.		

Programas sociales			
Datos de identificación			
Fecha de elaboración	Día	Mes	Año
	10	10	2021
Sujeto obligado	Jocotepec, Jalisco		
Unidad administrativa responsable	Dirección de economía Dirección de Desarrollo Rural Dirección de Desarrollo Social		
Contenido del Sistema			

Finalidad de sistemas y usos previstos	Seguimiento a los programas sociales organizados y dirigidos por la federación y el estado en beneficio de los habitantes del Municipio, y la organización, preparación y seguimiento de los programas sociales municipales.	
Las personas o grupos de personas sobre las cuales se obtienen los datos	Personas físicas que cumplan con los requisitos para ser beneficiarios de los programas	
Procedimiento de recolección	Formatos físicos.	
Tipo de soporte en donde se contienen los datos personales	Físicos y electrónicos.	
Características del lugar de resguardo	Archiveros, cajas o muebles dentro de las oficinas de cada área y en plataformas.	
Estructura básica del sistema y la descripción de los tipos de datos incluidos		
Datos generales del sistema		
Área	Responsable	Cargo
Departamento de Promoción Económica Dirección de Desarrollo Rural Dirección de Desarrollo Social		Departamento de Promoción Económica Director de Desarrollo Rural Director de Desarrollo Social
Domicilio	Teléfono	correo electrónico

Hidalgo sur 6	3877631919	promocioneconomica@jocotepec.gob.mx desarrollorural@jocotepec.gob.mx desarrollosocial@jocotepec.gob.mx
Administradores		
Area	Administradores	Cargo
Departamento de Promoción Económica Dirección de Desarrollo Rural Dirección de Desarrollo Social		Encargada Director Directora
Datos personales incluidos en el Sistema/Inventario		
Tipo de datos personales		
Nombre, edad, fecha de nacimiento, estado civil, nacionalidad, origen étnico, CURP, RFC, peso, altura, fotografías personales, información familiar, información de sus hijos (nombre, edad, estado de salud y/o discapacidad), información laboral, domicilio, teléfono, correo electrónico, estado civil, firma, datos socioeconómicos (pobreza alimentaria), estado de salud (enfermedades y/o discapacidades), información bancaria (clabe interbancaria, número de cuenta y/o tarjeta).		
Tipo de tratamiento	Tratamiento no automatizado y automatizado. El que requiera el trámite, siempre y cuando sea lícito, conforme a las nuevas medidas de seguridad.	
Cesión de las que puede ser objeto la información confidencial		
Unidades internas, sujetos obligados, autoridades o terceros a los que en su caso se ceden los datos		

Los Programas Sociales Municipales transfieren información de los beneficiarios a instituciones bancarias para efecto de tramitar una cuenta y/o tarjeta de débito.	Realizar las dispersiones de los apoyos económicos a los beneficiarios.	
En caso de programas sociales estatales y federales, se transfiere el listado de beneficiarios a los entes públicos federales que dirigen dichos programas sociales.	Dar cabal y oportuno seguimiento a los programas sociales federales y estatales aplicables en el ámbito municipal.	
Nivel de protección exigible El detalle podrá ser consultado en el inventario de trámites		Básico
		Medio
	X	Alto
Fundamento legal		
Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios Ley De Desarrollo Social Para El Estado De Jalisco Guía Para La Elaboración De Reglas De Operación Del Gobierno De Jalisco 2021		

Contratación de empleados o funcionarios			
Datos de identificación			
Fecha de elaboración	Día	Mes	Año
	10	10	2021
Sujeto obligado	Municipio de Jocotepec, Jalisco		
Unidad administrativa responsable	Dirección de Administración		
Contenido del Sistema			
Finalidad de sistemas y usos previstos	Dar inicio, seguimiento y conclusión a procedimientos internos que ayudan al correcto desempeño de la Administración Pública Municipal, la contratación de personal,		
Las personas o grupos de personas sobre las cuales se obtienen los datos	Servidores Públicos del Municipio de Jocotepec, Jalisco		
Procedimiento de recolección	Registro de captura de información proporcionada por servidores públicos		
Tipo de soporte en donde se contienen los datos personales	Los datos personales se encuentran en soporte físico y electrónico		
Características del lugar de resguardo	La información se encuentra resguardada en archivos dentro de una oficina específica, cuenta con seguridad como llave y se encuentran dentro de la oficina de Administración, misma que sólo se tiene acceso a ello el encargado de Expedientes personales.		

Estructura básica del sistema y la descripción de los tipos de datos incluidos		
Datos generales del sistema		
Area	Responsable	Cargo
Dirección de Administración		Director
Domicilio	Teléfono	Correo electrónico
Hidalgo sur 6	3877631919	administracion@jocotepec.gob.mx
Administradores		
Area	Administradores	Cargo
Recursos Humanos		Auxiliar Administrativo
Datos personales incluidos en el Sistema/Inventario		
Tipo de datos personales		
Nombre, edad, fecha de nacimiento, nacionalidad, RFC, CURP, fotografías personales, domicilio, teléfono, correo electrónico, estado civil, cuentas bancarias, firma, beneficiarios, datos que contiene credencial para votar, referencias personales, calificaciones académicas, y resultados médicos.		
Tipo de tratamiento	Tratamiento no automatizado y automatizado	
Cesión de las que puede ser objeto la información confidencial		
Sujetos obligados, autoridades o terceros a los que en su caso	Despacho Jurídico denominado "Servicios Especializados GACLO S.C.	

se ceden los datos.		
Nivel de protección exigible El detalle podrá ser consultado en el inventario de trámites		Básico
		Medio
	X	Alto
Fundamento legal		
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 Ley Para Los Servidores Públicos Del Estado De Jalisco Y Sus Municipios		

Inspección y vigilancia			
Datos de identificación			
Fecha de elaboración	Día	Mes	Año
	10	10	2021
Sujeto obligado	Municipio de Jocotepec, Jalisco		
Unidad administrativa responsable	Dirección de Padrón , Licencias y Reglamentos		
Contenido del Sistema			

Finalidad de sistemas y usos previstos	Control de datos personales recabados mediante reportes por oficio y documentación generada en campo.	
Las personas o grupos de personas sobre las cuales se obtienen los datos	Ciudadanos que acuden a realizar trámites.	
Procedimiento de recolección	Generados en campo por visitas de inspección y vigilancia.	
Tipo de soporte en donde se contienen los datos personales	El registro con el que se cuenta es documental, no en datos abiertos.	
Características del lugar de resguardo	Resguardados en archivos dentro de un archivero, de esta área el cual cuenta con seguridad como llave y está dentro de oficinas que solo personal autorizado tiene acceso.	
Estructura básica del sistema y la descripción de los tipos de datos incluidos		
Datos generales del sistema		
Area	Responsable	Cargo
Dirección de Padrón , Licencias y Reglamentos		Director
Domicilio	Teléfono	Correo electrónico
Hidalgo sur 189	3877632470	reglamentos@jocotepec.gob.mx padronylicencias@jocotepec.gob.mx
Administradores		
Area	Administradores	Cargo

Departamento de Inspectores		Encargado de Inspectores
Domicilio	Teléfono	Correo electrónico
Hidalgo sur 189	3877632470	reglamentos@jocotepec.gob.mx
Datos personales incluidos en el Sistema/Inventario		
Tipo de datos personales		
Domicilio particular, Nombre, Teléfono, Correo Electrónico.		
Tipo de tratamiento	Tratamiento no automatizado y automatizado.	
Cesión de las que puede ser objeto la información confidencial		
Unidades internas, sujetos obligados, autoridades o terceros a los que en su caso se ceden los datos	n/a	
El detalle podrá ser consultado en el inventario de trámites	Seguimiento y conclusión del trámite iniciado por el ciudadano.	
Nivel de protección exigible El detalle	**X**	Básico
		Medio

podrá ser consultado en el inventario de trámites		Alto
Fundamento legal		
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		

Registro de personas detenidas, lesionados y/o occisas			
Datos de identificación			
Fecha de elaboración	Día	Mes	Año
	10	10	2021
Sujeto obligado	Municipio de Jocotepec, Jalisco		
Unidad administrativa responsable	Dirección de Seguridad Pública		
Contenido del Sistema			
Finalidad de sistemas y usos previstos	Registro de datos de personas detenidas por la policía municipal, así como, lesionados y occisos en el municipio de Jocotepec, Jalisco en una base de datos especializada en la identificación de estructuras y modos de operación delincuencial, para su combate.		

Las personas o grupos de personas sobre las cuales se obtienen los datos	Detenidos, Lesionados y Familiares de Occisos.	
Procedimiento de recolección	Formatos digitales	
Tipo de soporte en donde se contienen los datos personales	Los datos personales se encuentran en soporte físico la mayoría de los expedientes y algunos electrónico.	
Características del lugar de resguardo	Resguardados en archivos y gavetas dentro de oficinas con llave y en plataformas.	
Estructura básica del sistema y la descripción de los tipos de datos incluidos		
Datos generales del sistema		
Area	Responsable	Cargo
Domicilio	Teléfono	Correo electrónico
Administradores		
Area	Administradores	Cargo
Domicilio	Teléfono	Correo electrónico

		-
Datos personales incluidos en el Sistema/Inventario		
Tipo de datos personales		
Nombre, Edad, Fecha de Nacimiento, Ocupación, Escolaridad, Estado Civil, Nombre de Progenitores, Domicilio y Fotografías Personales.		
Tipo de tratamiento	Tratamiento no automatizado y automatizado.	
Cesión de las que puede ser objeto la información confidencial		
Unidades internas, sujetos obligados, autoridades o terceros a los que en su caso se ceden los datos	n/a	
Nivel de protección exigible El detalle podrá ser consultado en el inventario de trámites		Básico
		Medio
	X	Alto
Fundamento legal		
Artículo 21, párrafos noveno y décimo de la Constitución Política de los Estados Unidos Mexicanos; Artículos 5, fracción II, 41, fracción I, 43, 112 y 113 de la Ley General del		

III. De las funciones y obligaciones de las personas que tratan datos personales

Para garantizar la aplicación correcta de este sistema es necesario establecer los deberes de los servidores públicos del municipio que participan en el tratamiento de los datos personales derivado de sus atribuciones.

Al momento de recibir los datos personales el servidor público que se encargue de su recepción deberá:

1) Tener a la vista el Aviso de Privacidad.

2) Dar a conocer el aviso de privacidad al titular de los datos personales previo a la obtención de sus datos.

3) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia de Jocotepec, Jalisco.

4) Al obtener los datos personales, cerciorarse de que la información esté completa, actualizada, sea veraz, y comprensible.

5) Comunicar discrepancias de los datos personales recabados a su jefe inmediato o al administrador de los datos personales, ello cuando se dé cuenta.

6) Conocer y seguir las medidas de seguridad que le sean aplicables para el cuidado de los datos personales, durante el periodo en el que posea los datos personales.

7) Recabar los datos personales para la finalidad para la cual estos fueron recabados según el trámite o el sistema de tratamiento que corresponda.

8) Tratar los datos personales de manera lícita siguiendo los principios establecidos

en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

9) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Jocotepec, en el tratamiento de datos personales.

10) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

11) Tomar, una vez al año un curso, taller o capacitación sobre el tratamiento de datos personales.

12) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

El servidor público involucrado en el tratamiento de datos personales deberá:

1) Conocer, aplicar y sujetarse al Aviso de Privacidad y al Documento de Seguridad del Gobierno Municipal de Jocotepec, en el tratamiento de datos personales.

2) Aplicar las medidas de seguridad correspondientes a los datos personales tratados y/o el sistema de protección en el que participa.

3) Tratar los datos personales de manera lícita siguiendo los principios establecidos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

4) En caso de dudas o quejas de los titulares de los datos personales sobre el tratamiento de sus datos, orientar al ciudadano para que acuda a la Unidad de Transparencia.

5) Guardar estricta confidencialidad de los datos personales que conozca en el ejercicio de sus funciones.

6) Abstenerse de realizar transferencias de datos personales que no vayan de conformidad con la finalidad para la cual se obtuvieron los datos.

7) Tomar, una vez al año, un curso, taller o capacitación sobre el tratamiento de datos personales.

8) Sujetarse a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco.

Son obligaciones de la Unidad de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 88 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:

1) Difundir al interior del Gobierno Municipal el aviso de privacidad y el documento de seguridad.
2) Revisión física anual a 2 dependencias sobre el tratamiento de datos personales y la implementación de medidas de seguridad.
3) Proponer al Comité de Transparencia actualizaciones o modificaciones al documento de seguridad.
4) Emitir un reporte anual al Comité de Transparencia sobre el ejercicio de estas funciones.

Son obligaciones del Comité de Transparencia en relación al tratamiento de datos personales, además de las previstas en el artículo 87 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco:
1) Revisar anualmente las políticas y/o lineamientos en materia de protección de datos personales establecidos en el presente documento.
2) Emitir o aprobar anualmente un programa de capacitaciones en materia de protección de datos personales.
3) Requerir anualmente a las dependencias o áreas responsables que tratan datos personales, a través de la DTB, informes sobre el tratamiento de los datos personales y la aplicación de medidas de seguridad, así como vulneraciones detectadas en el año.

La Contraloría de Jcootepec, Jalisco, conforme sus atribuciones establecidas en las _____ del Reglamento de la Administración Pública Municipal de Jocotepec,

Jalisco, podrá hacer revisiones o auditorías sobre la aplicación del presente documento de seguridad.

IV. Del análisis de riesgos

Debido a las circunstancias generales, tanto físicas como humanas, en las que se tratan datos personales, hemos logrado identificar los siguientes riesgos posibles ante los que se
pudiera enfrentar este Sujeto Obligado:

- Obtención de datos incompletos o incorrectos.
- Omitir la notificación al titular de los datos personales del aviso de privacidad.
- No difundir el aviso de privacidad.
- Ante la necesidad de tener un consentimiento expreso: no tener evidencia de que el titular de los datos personales conoce los términos del aviso de privacidad.
- No tener un lugar seguro y de acceso restringido en donde se puedan archivar los datos personales en físico.
- Permitir a todo servidor público o personas ajenas a la dependencia, el acceso a los expedientes que contienen datos personales.
- Daño de la base de datos que contenga información confidencial.
- Fallas en los equipos de cómputo en donde se encuentran las bases de datos.
- Falta de capacitación de los servidores públicos en relación a la confidencialidad que deben guardar sobre los datos personales que conozcan debido al desempeño de sus
funciones.
- Pérdida, robo o extravío de expedientes.
- Alteración de la información.

Ante dichos riesgos identificados es necesario hacer un análisis de dichos riesgos, amenazas y sus posibles vulneraciones.

Origen de la amenaza	Causa	Posibles consecuencias
Acceso de personas no autorizadas a los sistemas o plataformas oficiales del municipio	Adquirir información o datos personales	Acceso no autorizado. Divulgación de datos personales. Robo de información. Modificaciones no autorizadas. Robo de información
Acceso de personas no autorizadas como criminales o traficantes de datos a los sistemas o plataformas oficiales del municipio.	Adquirir datos personales para utilizarlos con fines de explotación, chantaje, extorsión o cualquier uso criminal.	Extorsiones. Ataques a personas, Robo de información. Vulneración a la seguridad física y mental de los ciudadanos. Robo de información
Personal del sujeto obligado con poco conocimiento sobre el tratamiento de datos personales	Obtener información para beneficio personal. Curiosidad. Error involuntario. Por fines económicos.	Ataque a otros servidores públicos. Robo de información. Pérdida de datos personales. Uso indebido de datos personales. Uso ilícito de datos personales. Robo de información. Extorsión. Modificaciones no autorizadas. Robo de información.
Daño físico	Agua Fuego, Accidentes, Corrosión	Daño o pérdida de los datos personales.

Eventos naturales	Desastres climatológicos, Fenómenos meteorológicos. Sismos, Cualquier eventualidad por causa natural	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas
Fallas técnicas	Pérdidas de electricidad. Falla o pérdida de internet. Falla en sistemas, Correos electrónicos o plataformas oficiales.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas.
Decadencias técnicas.	Mantenimiento insuficiente. Falla en equipos. Poca o absoluta renovación de equipos de telecomunicaciones o cómputos. Cambios de voltaje.	Pérdida, destrucción y daño.
Susceptibilidad en redes o sistemas autorizados.	Falta de contraseñas altamente efectivas. Falta de mecanismos para identificar o autenticación de usuarios. Falta de actualización de antivirus.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información. Robo de información.

Organización.	Procesos carentes de formalidad para administración, acceso, uso y proceso de archivo.	Pérdida, destrucción y daño. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información. Robo de información.
Espacio donde se archiven.	Carencia de espacio. Espacio con poca seguridad. Espacio no adecuado. Falta de llaves o medidas de seguridad para accesos.	Daño o pérdida de los datos personales. Divulgación y transferencia de datos personales. Modificaciones no autorizadas. Robo de información.

Daño y/o alteración de la base de datos que contenga información confidencial.	Carencia de un servidor o sistema que almacene los datos personales. La falta de registros, controles o bitácoras, para regular la entrada y salida de personal autorizado, al área donde se almacenan o archivan los datos personales (en su caso los expedientes que los contengan), es un escenario de vulneración y riesgo, facilitando el mal manejo de los datos personales y la pérdida, robo o extravío de expedientes.	Daño y/o pérdida de los datos personales. Modificaciones no autorizadas.

Hasta el momento no se han identificado o reportado vulneraciones desde las áreas

generadoras de información o las dependencias que integran el Gobierno Municipal de Jocotepec.

V. Del análisis de brecha

Una vez identificados los posibles riesgos a los que este Sujeto Obligado se encuentra
susceptible de enfrentar, podemos realizar el análisis de brecha, utilizando como base las
entrevistas que se hicieron con cada enlace que tiene la DTB con diferentes áreas del
Gobierno Municipal.

Las áreas administrativas reportaron las siguientes medidas de seguridad existentes:

- Quien recaba los datos personales, es un servidor público del área, asignado especialmente para recabar datos en general necesarios para cada trámite.
- El espacio físico o área donde se recaban datos personales, es dentro de las instalaciones.
- Cuando los datos personales son recabados de forma digital, se realiza por medio de plataformas oficiales o correo electrónico oficial.
- En la mayoría de las áreas, el acceso (al área donde se recibe a los ciudadanos y se
recaban datos personales) se tiene restringido, una vez que el dato se encuentra en posesión del servidor público, es decir si fue recabado frente a un escritorio, ventanilla, área abierta o pasillo, los ciudadanos no podrán pasar detrás de estos, ya que al terminar de recabar datos estos se colocan fuera del alcance de los ciudadanos.
- Cada oficina cuenta con puertas que separa el área al momento de terminar labores.
- Las llaves que se tienen de cada área se encuentran en manos de servidores públicos, autorizados por cada área.

● Una vez recabados los datos personales, el servidor público genera un expediente para cada trámite o servicio, del cual se obtuvieron los datos personales, ya sea físico o electrónico.

● Una vez recabados los datos personales, ya realizada la carpeta o expediente (electrónica, física, en plataformas, o cualquiera generada) y guardada esta en archiveros o puesta en resguardo electrónico, tienen acceso a esta área servidores públicos del área.

● Las llaves de los archiveros con las que se cuentan se encuentran en posesión de servidores públicos encargados del área.

● Una vez recabados los datos personales, en caso de que se les dé proceso electrónico, el servidor público guarda los mismos en carpeta electrónica, ya sea en su computadora, carpeta compartida, correo electrónico oficial o plataforma.

● Durante el desahogo del trámite del cual se obtuvieron los datos personales, los servidores públicos del área tienen acceso a los datos personales.

● Una vez concluido el trámite, los datos personales recabados se dejan intactos en la carpeta, archivo o expediente del trámite al que pertenecen.

● Cada carpeta de trámites o archivo, al terminar el proceso de cada uno, son resguardados en un archivo de cada área.

Las medidas de seguridad que actualmente se llevan a cabo pudieran ser efectivas de aplicarse de manera continua y consciente en las áreas administrativas del sujeto obligado El riesgo latente que se provoca por la falta de conocimiento, o compromiso para la aplicación de estas medidas existentes se puede minimizar por medio del establecimiento obligatorio de dichas medidas de seguridad y de la mejora continua de las mismas.

VI. De las medidas de seguridad

Con base en lo anterior se establecen las siguientes medidas de seguridad de carácter físico, técnico y administrativo:

Objetivo de control	Descripción
Control de servidores públicos que recaban los datos personales.	Debe realizarse un listado de los servidores públicos que recaban datos personales, esto es, de los servidores públicos que tienen contacto con el titular de los datos personales por sus funciones. (Quien recabe los datos generales para el trámite a realizar). Actualización del listado: cada 6 meses.
Control de servidores públicos que recaban los datos personales.	Forzosa asistencia a por lo menos a 1 capacitación en materia de datos personales impartida por la DTB.
Control de servidores públicos que recaban los datos personales.	Remitir el documento de seguridad para el conocimiento y cumplimiento de las medidas de seguridad aplicables para un correcto tratamiento de datos personales.
Obtención de datos.	Para evitar el riesgo de obtener datos personales incompletos o incorrectos, el servidor público autorizado para recabarlos, deberá pedir al ciudadano acredite su personalidad.
Aviso de privacidad.	El servidor público que reciba los datos personales, deberá tener a la vista de todos los ciudadanos el aviso de privacidad, y darlo a conocer al momento de la recepción del trámite.

Aviso de privacidad.	Si el trámite del cual se recabarán datos personales, cuenta con un formato, este deberá contener la mención y debe dar a conocer el aviso de privacidad del municipio, ya sea simplificado o la liga de internet que remita al ciudadano al aviso general. Los formatos nuevos que se impriman posteriores a la emisión del presente documento deberán contar con la liga al aviso de privacidad o en su defecto el aviso de privacidad simplificado.
Aviso de privacidad	Si el trámite del cual se recabarán datos personales, fue recabado mediante una plataforma electrónica oficial, esta plataforma deberá contener la mención y debe dar a conocer el aviso de privacidad del municipio, ya sea simplificado o la liga de internet que remita al ciudadano al aviso general.
Espacio físico.	Los datos personales recabados deberán ser recibidos únicamente en las instalaciones de cada área.
Espacio físico.	El área específica donde se recaben los datos deberá contar con puertas que tengan llave, sin excepción alguna, para asegurar de forma efectiva el trato adecuado de los datos personales, así evitar mal uso de los mismos o vulneraciones.
Espacio físico.	Las llaves de las puertas de cada dependencia, deberán ser guardadas únicamente por servidores públicos del área, autorizados para poseer las llaves.
Espacio físico.	Al término de las labores, deberá cerrarse cada oficina de las áreas, para evitar el contacto de otros servidores públicos o ciudadanos con los datos personales recabados.

Espacio físico.	Al concluir la jornada laboral, se deberá guardar los expedientes, para no dejarlos al alcance de ciudadanos o personal no autorizado.
Resguardo provisional, durante el desahogo del trámite	Una vez recabados los datos personales, al generar el expediente (derivado del trámite), este deberá ponerse en algún lugar que esté fuera del alcance de los ciudadanos, ya sea en una caja, archivero, o mueble.
Archivo, al finalizar el desahogo del trámite	Al finalizar el desahogo de los expedientes estos deberán archivarse en un lugar adecuado con las siguientes características: · No estar al alcance de los ciudadanos o servidores públicos ajenos al área. · Deberá ser un área específica para guardar los expedientes. · Este archivo debe estar bajo llave. · La llave del mismo solo puede estar en manos de un servidor autorizado para esto.

Acceso al archivo.	Se deberá crear por cada área, un control o bitácora de los servidores públicos que tienen acceso al archivo, el control debe contener lo siguiente: · Registro para anotar el nombre y puesto del servidor público autorizado. · Fecha, hora de entrada y hora de salida del archivo. · Registrar el expediente que se consultó. · Registrar el expediente que se extrae del archivo, y fecha en la que se regresa el expediente. · Firma de conformidad del servidor público que entró. · Firma de consentimiento del servidor público autorizado para llevar el control de este archivo.
Control de archivos electrónicos.	Cuando los datos personales sean recabados por medios electrónicos, se deberá generar expediente por cada trámite, dicho expediente deberá ser guardado en base de datos, correo electrónico oficial, o en plataforma autorizada, no en cualquier plataforma o correo electrónico personal.
Control de archivos electrónicos.	Para evitar riesgos, respecto a los expedientes electrónicos, se debe contar con un respaldo electrónico. Dicho respaldo deberá realizarse, como mínimo, de manera anual.
Inventarios Documentales sobre archivos entregados a la Dirección de Archivos.	Cada área del sujeto obligado deberá elaborar controles de archivo, conforme a sus procesos institucionales. Esto es, un inventario de documentos que se mandan a la Dirección de Archivo para su resguardo en el Archivo Municipal.

Transferencia de datos personales.	En caso de ser necesario derivado de las funciones de los servidores públicos, o por requisito del trámite, se deba realizar una transferencia de datos personales, se deberá informar al sujeto que reciba los datos el aviso de privacidad para que se sujete al mismo.
Versiones Públicas	En los casos en los cuales se realicen clasificaciones de información confidencial, que incluyan datos personales, los documentos que contengan los datos, deberán entregarse siempre en versión pública, adjuntando índice de datos personales. Archivo finalizado Al momento de finalizar el trámite, todos los expedientes
Archivo finalizado	Al momento de finalizar el trámite, todos los expedientes, deberán desecharse y enviarse y mandarse al archivo municipal, conforme a la normatividad correspondiente.

Medidas de seguridad para transferencias:

Transferencias al interior del sujeto obligado y a otros sujetos obligados:

- Solo podrán ser transferidos los datos personales para dar seguimiento y conclusión al trámite o sistema de tratamiento bajo la finalidad que éstos prevean.

- El área que entrega los datos personales deberá cerciorarse de transferir la totalidad de los datos que resulten necesarios para el seguimiento o la conclusión del trámite o sistema de tratamiento correspondiente. Limitándose a la entrega de datos adicionales que no resulten necesarios.
- El área que entrega los datos personales deberá cerciorarse de que los datos que transfiere sean completos y veraces.
- El área que reciba los datos personales deberá conservar los mismos sujetándose a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y adoptando las medidas de seguridad previstas en este documento.
- El área que reciba los datos personales deberá encargarse de la supresión de los datos que reciba cuando esta corresponda.
- El área que entrega y el área que recibe los datos personales deberán dar acceso a los datos personales en tratándose de procedimientos de derecho ARCO.

Transferencias a terceros:

- El tercero que reciba los datos personales deberá sujetarse a las finalidades y lineamientos del aviso de privacidad de este sujeto obligado y deberá adoptar las medidas de seguridad previstas en este documento.
- En caso de ser necesario conforme a las disposiciones normativas, se deberá firmar un convenio o acuerdo de confidencialidad que proteja el tratamiento de los datos personales que recaba este sujeto obligado y transfiere al tercero.

Medidas de seguridad en caso de vulneraciones a la seguridad:

En caso de ocurrir alguna vulneración deberá registrarse en la bitácora de contingencias,

misma que deberá seguirse bajo el siguiente formato y ejemplo:

Fecha en la que ocurrió	Motivo	Las acciones correctivas implementadas de formas inmediatas y definitivas
30/08/2021	Tromba	Impresión del expediente. Generar nuevo expediente electrónico

Después del registro, se deberá informar de forma inmediata al titular y al instituto las vulneraciones de seguridad ocurridas, las que afecten o impacten de forma significativa los derechos patrimoniales o morales del titular, en un plazo máximo de setenta y dos horas en cuanto se confirmen y este en proceso las acciones encaminadas para dimensionar la afectación, con la finalidad de que los titulares puedan tomar medidas correspondientes para la defensa de sus derechos, dicha notificación debe contener lo siguiente:

I. La naturaleza del incidente.
II. Los datos personales comprometidos.
III. Las recomendaciones y medidas que el titular puede adoptar para proteger sus intereses.
IV. Las acciones correctivas realizadas de forma inmediata.
V. Los medios donde puede obtener mayor información al respecto.
Al ocurrir una vulneración de seguridad, el servidor público titular del área responsable y/o el responsable del sistema deberá analizar la causa por lo que

ocurrió dicha vulneración, e implementar y anexar a su plan de trabajo las acciones preventivas y correctivas para adecuar medidas de seguridad que prevengan esta eventualidad, para evitar que la vulneración se repita. A su vez, en caso de detectar que la falla fue ocasionada por el incumplimiento de un servidor público a su cargo deberá levantar acta circunstanciada de hechos correspondiente y seguir el procedimiento administrativo correspondiente ante la Contraloría Municipal.

Medidas de seguridad o controles para la identificación y autentificación de usuarios:

Parte de tener control efectivo al trato de los datos personales es contar con un sistema que garantice la autenticación de usuarios, esto es por medio de administración de cuentas creadas específicamente para cada servidor público.

La administración de cuentas de usuario es una parte esencial de los sistemas que se desarrollan en el departamento de software. La razón principal de las cuentas de usuario es verificar la identidad de cada funcionario también permite la utilización personalizada de acceso a la información y generación de la misma.

Esta medida es tomada para los correos electrónicos institucionales y para cualquier sistema o plataforma tecnológica que cree este sujeto obligado.

El estándar para la creación de las cuentas es:

Usuario: Generalmente es el correo electrónico institucional

Contraseña: Frase de confirmación de identidad que se encuentra encriptada para mayor seguridad.

Estos accesos son dados, por parte de la Dirección de Innovación del Gobierno Municipal de Jocotepec, Jalisco, mediante una carta responsiva personalizada la cual va firmada por el interesado y la persona que autoriza. Dicha carta se anexa a continuación:

Medidas de seguridad para la supresión y borrado seguro de datos personales:

Todos los datos personales en posesión del sujeto obligado sin importar el soporte en el que se encuentren deberán ser tratados para la supresión y borrado conforme a lo establecido en el Manual de procedimientos de Secretaría General y la Dirección

de Archivo Municipal, ya que el mismo tiene como uno de sus propósitos ser una guía para la operación de eliminación de archivos.

De conformidad con el artículo 3 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Jalisco y sus Municipios fracción V, el bloqueo se dará únicamente después del cumplimiento de la finalidad con la que fueron recabados los datos personales hasta que cumpla el plazo de prescripción legal o contractual correspondiente, concluido éste se deberá proceder a la supresión en la base de datos, archivo, registro, expediente que corresponda, al mismo tiempo se está garantizando la supresión de los datos personales.

Ahora bien especificaremos los objetivos de contar con técnicas apropiadas para la supresión y borrado de datos personales:

· Que la supresión y borrado de los expedientes que contengan datos personales sea de forma legal.

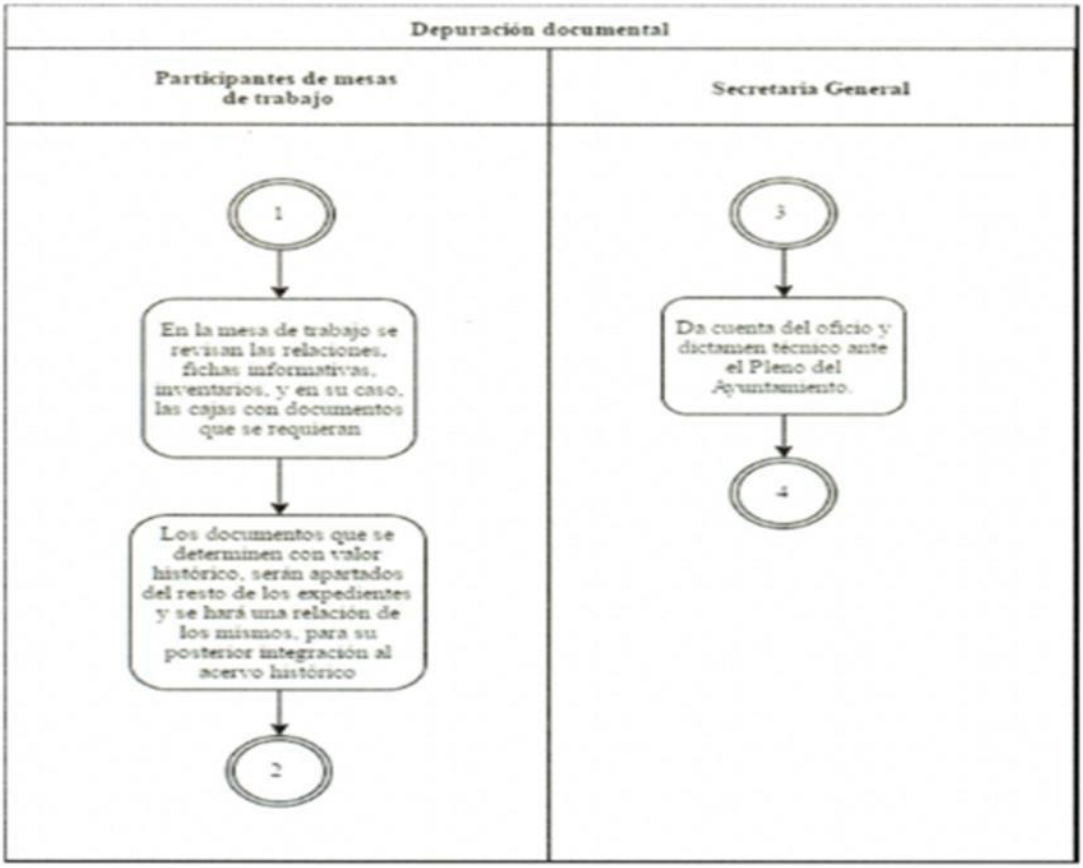
· Que la supresión y borrado de los expedientes que contengan datos personales sea de forma operativa conforme a los procedimientos utilizados en el municipio.

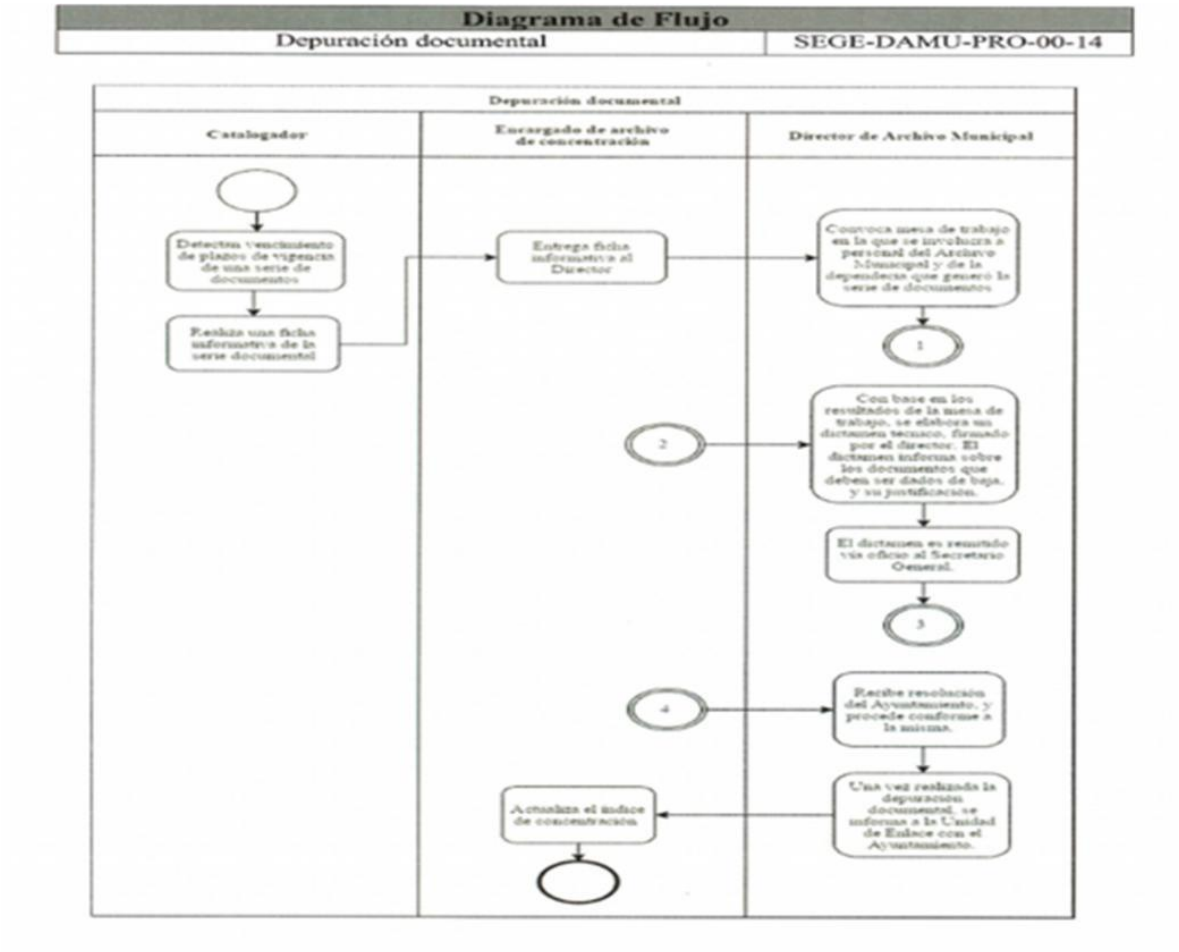
· Servir como base para el proceso adecuado de supresión y borrado de los expedientes que contengan datos personales.

· Guía para depuración de datos personales.

Este apartado es el conjunto de estructuras para el proceso de supresión y borrado de los expedientes que contengan datos personales en posesión del sujeto obligado; por lo tanto los datos personales deberán estar contenidos en archivos apegados a un orden lógico y cronológico.

De conformidad con el Manual de procedimientos de Secretaría General y la Dirección de Archivo Municipal el proceso de depuración es el siguiente, mismo que será aplicado para datos personales:


Depuración documental
Participantes de mesas de trabajo
Secretaría General
1
En la mesa de trabajo se revisan las relaciones, fichas informativas, inventarios, y en su caso, las cajas con documentos que se requieran
Los documentos que se determinen con valor histórico, serán apartados del resto de los expedientes y se hará una relación de los mismos, para su posterior integración al acervo histórico
2
3
Da cuenta del oficio y dictamen técnico ante el Pleno del Ayuntamiento.
4



Bases para supresión y borrado seguro de archivos:

· Las bajas documentales se realizan mediante la aprobación del pleno del Ayuntamiento.

· Los documentos físicos cuya baja ha sido procedente, se entregan a un reciclador. Los documentos son vigilados por personal del Gobierno Municipal hasta su destino final,

en donde son triturados.

· De acuerdo a la Ley que Regula la Administración de los Documentos Públicos e Históricos del Estado de Jalisco, los documentos dados de baja cuentan con una antigüedad mayor a los 10 (diez) años, y ya no cuentan con ningún tipo de vigencia ni validez alguna.

Como referencia para la adecuada técnica de supresión y borrado seguro de los datos personales se tomará en todo momento como base lo siguiente:

· Acuerdo A 04/2015-2018, mediante el cual se ordena la habilitación de una mesa de trabajo que brinde apoyo a la Dirección de Archivo Municipal para la elaboración del dictamen técnico de depuración documental.

· Acuerdos que autorizan la depuración de documentos (se adjunta la publicación de dos de ellos como muestra de este tipo de resoluciones).

VII. Del plan de contingencia:

Ante la pérdida total o parcial de datos personales en posesión de este sujeto obligado, se debe contar con un plan de contingencia.

Con la evaluación de riesgos y la elaboración de las medidas de seguridad aplicables para prevenir las posibles vulneraciones a las que nos encontramos expuestos, nos encontramos con que el plan de contingencias de este sujeto obligado consiste en la aplicación de las medidas de seguridad tratadas en el apartado anterior, mismas que están sujetas a cambios por eventualidades no contempladas, por ello la importancia de señalar que el presente se trata de un plan de contingencia no limitativo.

Lo anterior toda vez que en la actualidad existen cambios y grandes avances que van modificando la organización de la información, y al igual existan riesgos inminentes que día a día evolucionan. Con la aplicación de las medidas de seguridad establecidas en este documento se buscan minimizar los riesgos o vulneraciones, pero a su vez se intenta propiciar el restablecimiento de los datos personales en el menor tiempo posible ante cualquier eventualidad.

En caso de que los datos personales sufran algún tipo de daño o pérdida, se dispondrá de los respaldos electrónicos realizados por cada área administrativa en donde se contienen copias de documentos y/o archivos y/o bases de datos que contienen datos personales que permitirían restablecer los datos a la fecha del último respaldo.

VIII. Del plan de trabajo:

La existencia del documento de seguridad, busca enmarcar los deberes del Municipio de Jocotepec, Jalisco para la máxima protección de datos personales. Debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

La finalidad de este plan es plasmar de manera enunciativa, más no limitativa, las actividades que el Municipio de Jocotepec, Jalisco realizará para la aplicación del resente documento de seguridad.

Lo anterior se realizará en base a las atribuciones establecidas en el la Ley de Protección de Datos Personales en Posesión de sujetos Obligados del Estado de Jalisco y sus Municipios.

Para la ejecución del presente documento de seguridad, dentro de los 6 meses siguientes a la emisión del presente documento:

1. Se emitirá circular para difundir la emisión del presente documento, a través de la cual se remitirá copia digital del mismo a todos los correos institucionales vigentes.
2. Se comunicará a los enlaces sobre la emisión del documento de seguridad, solicitando su apoyo para la difusión interna del mismo.
3. Se buscará la participación del ITEI para una primera capacitación básica para los servidores públicos que recaban datos personales.

El Comité de Transparencia revisará de manera anual, a partir de la emisión del presente documento de seguridad:

1. Revisar lo concerniente al índice de Datos Personales y mantenerlo actualizado.
2. Actualizar las medidas de Seguridad conforme al Sistema de Protección de Datos Personales hecho para el Municipio de Jocotepec, Jalisco.
3. Actualizar el presente plan de trabajo.
4. Se emitirá un programa anual de capacitaciones y además se promoverá

que el personal del Municipio de Jocotepec, Jalisco, se mantenga capacitado no sólo por sus áreas internas, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

XVI. Los mecanismos de monitoreo y revisión de las medidas de seguridad

Se debe realizar un monitoreo y revisión de la aplicación de las medidas de seguridad, para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización. Esto con el objetivo de que las medidas de seguridad continúan siendo efectivas e idóneas para el municipio.

Realizaremos el siguiente cuadro, donde se concentran los mecanismos de monitoreo y el objetivo de cada uno de ellos:

Mecanismos de monitoreo. Objetivo del monitoreo	**Objetivo del monitoreo**
Visita a 2 áreas cada 12 meses, las áreas serán elegidas de forma aleatoria	Verificar de primera mano la aplicación actualización e impacto de las medidas de seguridad aplicadas
Pedir reportes a los responsables de cada área generadora de información o a los responsables del sistema de datos persoanles o a sus administradores sobre el manejo de datos personales conforme a las medidas de seguridad	Monitorear avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad

XVII. El programa general de capacitación

Se manejaran las capacitaciones de conformidad con las necesidades del sujeto obligado en cuanto a la implementación y aplicación del sistema de manejo de datos personales, en posesión del sujeto obligado.

Las fechas exactas se les notificaran a los Enlaces de Transparencia con al menos una semana de anticipación a las fechas estimadas con la intención de que estos las difundan con los interesados en asistir a las capacitaciones.

SERVIDORES PÚBLICOS.

Protección de Datos Personales.- En esta capacitación se introducira a las novedades que brindara la Ley General de Proteccion de Datos Personales para poder realizar y administrar correctamente las gestiones y tramites que contienen información confidencial, así como las medidas que deben tomarse para su protección y las implicaciones que existen en caso de no proteger adecuadamente dicha información. Este módulo de capacitación se recomienda para todos los servidores públicos que manejan datos personales.

SERVIDORES PÚBLICOS.

Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios. - Este módulo está dirigido para el personal interesado en aprender lo mas básico en de protección de datos personales en apego a la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios. Teniendo como objetivo principal introducir a las bases y generalidades de esta nueva ley, así como resolver dudas de la misma.

SERVIDORES PÚBLICOS.

Medidas de Seguridad de Datos Personales. - En esta capacitación se introducirá a las novedades que brindará la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios para poder realizar y administrar correctamente las gestiones y tramites que contienen información confidencial, así como las medidas que deben tomarse para su protección. Este módulo de capacitación se recomienda para todos los servidores públicos que manejan datos personales.

SERVIDORES PÚBLICOS.

Versiones Públicas. - En este módulo se expondrán de manera general los lineamientos que el Sistema Nacional ha desarrollado para la correcta gestión de versiones públicas de documentos que serán entregados o publicados que contengan datos personales y su correcta realización, teniendo como objetivo principal explicar cómo se realiza una versión publica de los documentos que lo requieren y responder dudas sobre el tema que tengan los enlaces de transparencia.

SERVIDORES PÚBLICOS.

SISTEMA DE MANEJO DE PROTECCIÓN DE DATOS PERSONALES. - En este modulo se expondrán de manera general los lineamientos que el Sistema de manejo de datos personales en posesión del sujeto obligado, desarrollado para dar a conocer los nuevos lineamientos con respecto a este sistema, teniendo como objetivo principal explicar cómo se realizan las nuevas actividades que nos permitan desarrollar de forma precisa este sistema.

SERVIDORES PÚBLICOS.

SEGUIMIENTO DE MEDIDAS DE SEGURIDAD. - En esta capacitación se dará seguimiento a la aplicación de medidas de seguridad en cumplimiento a la Ley General de Protección de Datos Personales para poder realizar y administrar correctamente las mismas para el debido manejo de datos personales en posesión del sujeto obligado, así como las implicaciones que existen en caso de no proteger adecuadamente dicha información. Este módulo de capacitación se recomienda para todos los servidores públicos que manejan datos personales.

SERVIDORES PÚBLICOS.

SOLICITUDES DE ACCESO, RATIFICACIÓN, CANCELACIÓN U OPOSICIÓN DE DATOS PERSONALES. - Este módulo está dirigido para el personal del municipio que maneja datos personales y/o enlaces de transparencia de cada área

que da respuesta a las solicitudes de Derechos ARCO, esta capacitación tiene como finalidad instruir a los interesados como deben ser contestadas dichas solicitudes con base a la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios. Teniendo como objetivo principal introducir a las bases y generalidades de esta ley, así como resolver dudas de la misma.

SERVIDORES PÚBLICOS.

SESIÓN DE DUDAS EN MATERIA DEL ADECUADO MANEJO DE DATOS PERSONALES. - En este módulo se expondrán de manera general las posibles actualizaciones del documento de seguridad del sujeto obligado y se atenderán las dudas de los enlaces en materia de transparencia de cada área, para dar seguimiento y cumplimiento a la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Jalisco y sus Municipios