Salud
Secretaría de Salud



DOCUMENTO DE SEGURIDAD PARA EL PROCESO INTERNO DE LA DIRECCIÓN DE GESTIÓN DE PETICIONES CIUDADANAS Y PROMOCIÓN SOCIAL



2026
año de
Margarita
Maza



Índice

DATOS GENERALES DEL DOCUMENTO DE SEGURIDAD 3

ANTECEDENTES 4

I. EL INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO..... 5

II. LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES..... 19

III. EL ANÁLISIS DE RIESGOS 21

IV. EL ANÁLISIS DE BRECHA 22

V. PLAN DE TRABAJO 23

VI. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD..... 23

VII. PROGRAMA GENERAL DE CAPACITACIÓN..... 33

ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD 38



DATOS GENERALES DEL DOCUMENTO DE SEGURIDAD

NOMBRE
Documento de Seguridad para el Proceso Interno de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social.

UNIDAD ADMINISTRATIVA RESPONSABLE
Unidad Coordinadora de Vinculación y Participación Social, a través de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social.

SOPORTE DE ACTIVOS PARA EL TRATAMIENTO
Mixto (físico y electrónico).

FECHA DE ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD
15 DE JUNIO DE 2026.

Elaboró	Lic. Rodolfo Morales Pérez, Soporte Administrativo.
Aprobó	Mtra. Verónica Pinal González, Directora de Gestión de Peticiones Ciudadanas y Promoción Social



ANTECEDENTES

La elaboración del presente documento se fundamenta con lo establecido en los artículos 25, 26, 27, 28, 29 y 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como los artículos 55, 57, 58, 59, 60, 61, 62, 63 y 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público que corresponden a la elaboración del documento de seguridad.

Asimismo, de conformidad con el artículo 8º de la Constitución Política de los Estados Unidos Mexicanos por el que se consagra el derecho de petición; el artículo 14, fracción VI del Reglamento Interior de la Secretaría de Salud que corresponde a diseñar, implementar y dar seguimiento a los mecanismos y acciones necesarias para la debida gestión de las peticiones ciudadanas que se presenten en la Secretaría, con el fin de que las áreas competentes brinden de manera oportuna y eficiente la atención que corresponda.

El documento de seguridad es un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad físicas, técnicas y administrativas con las que el responsable garantiza la confidencialidad, integridad y disponibilidad de los datos personales que recaba y da tratamiento, contra la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado, o el daño, la alteración o modificación no autorizada.

La Unidad Coordinadora de Vinculación y Participación Social, por conducto de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social, es la responsable del tratamiento de los datos personales proporcionados, los cuales se encuentran protegidos conforme a lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en los Lineamientos Generales de Protección de Datos Personales para el Sector Público y demás normatividad aplicable.





I. EL INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

Este apartado describe la información básica del tratamiento de los datos personales, relacionada con la categoría de los tipos de datos (sensibles o no), el catálogo de soportes (físicos y automatizados) mediante los que se recaban y resguardan, así como su ubicación, las finalidades del tratamiento, las personas servidoras públicas que tienen acceso y sus posibles transferencias, lo anterior con fundamento en los artículos 27, fracción III y 29, fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 58 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, los cuales establecen que:

[…]

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

Artículo 27. *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*

[…]

III. *Elaborar un inventario de datos personales y de los sistemas de tratamiento;*

[…]

Artículo 29. *El responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*

I. *El inventario de datos personales y de los sistemas de tratamiento;*

[…]

LINEAMIENTOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR PÚBLICO

Artículo 58. *Con relación a lo previsto en el artículo 33, fracción III de la Ley General el responsable deberá elaborar un inventario con la información básica de cada tratamiento de datos personales, considerando, al menos, los siguientes elementos:*

I. *El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;*

II. *Las finalidades de cada tratamiento de datos personales;*

III. *El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;*

IV. *El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;*

V. *La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;*

VI. *En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y*





VII. *En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.*

[…]

Asimismo, el fundamento jurídico por el cual se establecen las atribuciones de esta Dirección de Gestión de Peticiones Ciudadanas y Promoción Social para realizar el tratamiento de los datos personales se encuentra en el artículo 8 de la Constitución Política de los Estados Unidos Mexicanos, referente al derecho de petición, así como el artículo 14, fracción VI del Reglamento Interior de la Secretaría de Salud, como se señala a continuación:

[…]

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

Artículo 8o. *Los funcionarios y empleados públicos respetarán el ejercicio del derecho de petición, siempre que ésta se formule por escrito, de manera pacífica y respetuosa; pero en materia política sólo podrán hacer uso de ese derecho los ciudadanos de la República.*

A toda petición deberá recaer un acuerdo escrito de la autoridad a quien se haya dirigido, la cual tiene obligación de hacerlo conocer en breve término al peticionario.

REGLAMENTO INTERIOR DE LA SECRETARÍA DE SALUD

Artículo 14. Corresponde a la Unidad Coordinadora de Vinculación y Participación Social:

[…]

VI. Diseñar, implementar y dar seguimiento a los mecanismos y acciones necesarias para la debida gestión de las peticiones ciudadanas que se presenten en la Secretaría, con el fin de que las áreas competentes brinden de manera oportuna y eficiente la atención que corresponda;

[…]

a) Catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales

Medios físicos y electrónicos a través de los cuales se obtienen los datos personales	
Plataforma en página web	• Sistema de Atención Ciudadana de la Presidencia (SACP): www.atencionciudadana.presidencia.gob.mx • Sistema de Administración de Correspondencia (SAC Salud): www.sac.salud.gob.mx/ • Contacto ciudadano: https://www.contactociudadanossa.atdt.gob.mx/





Correo electrónico	• Oficina del C. Secretario de Salud • Cámara de Diputados • Cámara de Senadores • Unidad Coordinadora de Vinculación y Participación Social • Dirección de Gestión de Peticiones Ciudadanas y Promoción Social
Físicos	• Presencial por el ciudadano

b) Finalidades del tratamiento de datos personales

La Dirección de Gestión de Peticiones Ciudadanas y Promoción Social tiene como objeto vincular y dar seguimiento oportuno a las peticiones ciudadanas que se realicen con la finalidad de ejercer su derecho de petición de acuerdo a lo establecido en el artículo 8° Constitucional.

Los datos personales son utilizados con la finalidad de llevar a cabo todas aquellas acciones necesarias para vincular y dar seguimiento a las solicitudes ingresadas a la Secretaría de Salud.

Una vez recabados los datos personales para la vinculación de la petición ciudadana, el asunto se remite al área competente mediante correo electrónico o, en su caso, a través de oficio. Para consulta y seguimiento, la información se registra en el Sistema Integral de Gestión Ciudadana (SIGC). Posteriormente, con el registro en el SIGC, se integra el expediente físico, el cual se identifica con un número consecutivo automatizado y las siglas correspondientes al área de recepción.

El personal de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social, no toma ni registra datos adicionales a los descritos en el catálogo.

c) Catálogo de los tipos de datos personales que se traten

Los datos personales que se recaban en la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social son de carácter identificativos y sensibles, siendo categorizados de la siguiente manera:



Identificativos	Sensibles
• Nombre completo del titular • Domicilio • Número telefónico fijo o de celular • Correo electrónico • Edad • Nombre de la persona responsable de brindar los datos, en caso de que el peticionario se encuentre imposibilitado para proporcionar la información	• Estado de salud presente o futuro • Padecimiento • Afiliación a servicio médico • Centro de salud o unidad médica hospitalaria de adscripción • Origen racial y étnico • Discapacidad • Afinidad religiosa • Condición socioeconómica • Ocupación • Situación migratoria • Identidad de género • Identidad de sexo

d) Catálogo de formatos de almacenamiento

A su vez, el catálogo de los tipos de datos personales debe establecer los siguientes elementos:

- **El formato en el que se encuentra la base de datos**: Es decir, el formato en que se obtienen los datos personales, como un formulario impreso en hojas de papel donde se registran los datos, copias de identificación de los titulares, formularios digitales, etc.

- **La ubicación de la base de datos:** Referir una descripción general de la ubicación física o resguardo de los activos de apoyo en los que se encuentran los datos personales.

- **Clasificación archivística:** La clasificación de los archivos que permite un mejor manejo de dichos activos, de acuerdo con el Listado General de Tipos Documentales, Tratamiento y Disposición Final de los Documentos de Comprobación Administrativa Inmediata, contenido en el Cuadro General de Clasificación Archivística y Catálogo de Disposición Documental de esta Secretaría de Salud.





Dato personal	Formato	Ubicación de la base de datos	Clasificación archivística
Datos Personales			
Nombre completo del titular	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Domicilio	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo





Número telefónico fijo o de celular	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Correo electrónico	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Edad	**Electrónicos**		





	- Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Nombre de la persona responsable de brindar los datos, en caso de que el titular esté imposibilitado de brindarlos	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Datos Personales Sensibles			
Estado de salud presente o futuro	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP)		





	- Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Padecimiento	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Afiliación a servicio médico	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud)	- Sistema Integral de Gestión Ciudadana	Documentos de Comprobación





	- Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	(SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Centro de salud o unidad médica hospitalaria de adscripción	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Origen racial y étnico	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de





	Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)		apoyo informativo
Discapacidad	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Afinidad religiosa	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos**	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo





	- Contacto ciudadano		
Condición socioeconómica	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Ocupación	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Situación migratoria	**Electrónicos**		





	- Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Identidad de género	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP) - Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo
Identidad de sexo	**Electrónicos** - Sistema de Atención Ciudadana de la Presidencia (SACP)		





	- Sistema de Administración de Correspondencia (SAC Salud) - Correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) **Físicos** - Contacto ciudadano (Recabados directamente la persona Titular)	- Sistema Integral de Gestión Ciudadana (SIGC) - Sistema interno de la DGPCPS - Expedientes físicos	Documentos de Comprobación Administrativa Inmediata (13) Copias fotostáticas de documentos de apoyo informativo

e) Servidores públicos que tienen acceso a los sistemas de tratamiento

La operación y administración del Sistema Integral de Gestión Ciudadana se lleva a cabo a través de un Responsable, dos Encargados y Usuarios.

- Responsable (electrónico/físico): Titular de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social.

- Encargado (electrónico): Soporte Administrativo de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social (Personal operativo).

- Encargado (físico): Soporte Administrativo de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social (Personal operativo).

- Usuarios (electrónico y físico), Soportes Administrativos (Personal operativo).

- Apoyos Administrativos (Personal operativo).

- Apoyo técnico (Electrónico), Soporte Administrativo de la Subdirección de Administración de Desarrollo de Personal e Informática.

f) Nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable

El tratamiento de los datos personales recabados en esta Dirección de Gestión de Peticiones Ciudadanas y Promoción Social se efectúa entre los responsables ya descritos en el punto anterior, sin necesidad de la interferencia de encargados.



g) Destinatarios o terceros receptores de las transferencias que se efectúen y sus finalidades

Se informa que se realizará la transferencia de datos personales y sensibles a las diferentes Unidades Administrativas de la Secretaría de Salud, a sus Órganos Desconcentrados, a los Institutos Nacionales de Salud, Hospitales Federales de Referencia y demás instancias del Sector Salud, así como a las Secretarías Estatales de Salud y, cuando el caso amerite, a las Coordinaciones Estatales del IMSS-Bienestar, según corresponda, para proceder a dar atención a la petición ciudadana. Asimismo, las transferencias de datos que realiza el área no requieren del consentimiento de los titulares de conformidad con los artículos 16, fracciones II y V, 59, 60, fracción I, 61 y 64, fracciones II y V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Asimismo, quedan a salvo sus derechos para poder transferir sus datos personales a los siguientes sujetos obligados en caso de que usted lo crea necesario:

- Comisión Nacional de Derechos Humanos: para la investigación de presuntas violaciones a derechos humanos

- Órganos Jurisdiccionales Federales (tribunales, juzgados, etc.): para la sustanciación de los procesos jurisdiccionales tramitados ante ellos

h) Ciclo de vida de los datos personales

1) **Obtención:** Se obtienen por medios electrónicos como el Sistema de Atención Ciudadana de la Presidencia (SACP), Sistema de Administración de Correspondencia (SAC Salud)**,** correos electrónicos institucionales (Cámara de Senadores, Cámara de Diputados, otras instituciones) y físicos a través del contacto ciudadano (Directamente de la persona titular).

2) **Almacenamiento:** Una vez que el solicitante proporciona sus datos y se realiza el llenado del Formato de Verificación de Datos de Peticionarios, se captura el nombre y la descripción de la petición en el Sistema Integral de Gestión Ciudadana, en el que se proporciona un número de expediente de acuerdo a su clasificación. El registro digital y expediente físico tienen una temporalidad de hasta 1 año, tiempo necesario para gestionar y dar seguimiento a la petición. Respecto al resguardo digital como medio de consulta y en cuanto al resguardo físico, cubre posibles aclaraciones posterior a la conclusión de la misma.

   El resguardo electrónico de los datos personales data de computadoras, servidores de correo electrónico, bases de datos y carpetas compartidas en la nube. En cuanto al SIGC, se trata de un programa en las computadoras del personal autorizado para el tratamiento de los datos personales.



El resguardo físico de los expedientes data de archiveros, gavetas y cajas que se mantienen bajo llave en el archivo de trámite de la Unidad.

3) **Uso de datos personales y divulgación:** La información proporcionada por el solicitante es será utilizada para dar trámite a su petición y es su vinculación canalizada al área competente para su resolución, la transferencia de estos datos se requiere únicamente para realizar la gestión y seguimiento de las peticiones.

   Una vez fenecido el plazo de conservación de las documentales generadas por la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social, se bloquea el tratamiento de los datos personales y personales sensibles durante un año y se procede a su respectiva supresión.

   La supresión definitiva de los datos personales resguardados se realiza al año de trabajo siguiente de acuerdo con su clasificación en el Listado General de Tipos Documentales, Tratamiento y Disposición Final de los Documentos de Comprobación Administrativa Inmediata, contenido en el Cuadro General de Clasificación Archivística y Catálogo de Disposición Documental de esta Secretaría de Salud.

   Lo anterior, toda vez que, de acuerdo con su clasificación, se trata de copias fotostáticas de documentos de apoyo informativo, por lo que carece de conceptos como vigencia o valores administrativos, de forma que no se transfieren al archivo de concentración y se realiza su baja un año después de su generación o al término de su utilidad.

Para mayor referencia, consultar lo descrito en el anexo de Inventario de Tratamientos (Anexo 1).

II. LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

Las funciones y obligaciones de las personas que traten datos personales encuentran su fundamento en lo establecido en los artículos 27, fracción II, 29, fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 57 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, que al pie de la letra señalan que:

[…]

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

Artículo 27. *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*





[…]

II. *Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;*

[…]

Artículo 29. *El responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*

[…]

II. *Las funciones y obligaciones de las personas que traten datos personales;*

[…]

Artículo 31. *En caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.*

LINEAMIENTOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR PÚBLICO

Artículo 57. *Con relación a lo dispuesto en el artículo 33, fracción 11 de la Ley General, el responsable deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.*

El responsable deberá establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales en su organización, conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.

[…]

Por lo anterior, las personas servidoras públicas que tratan datos personales en esta Dirección de gestión de Peticiones Ciudadanas y Promoción Social son:

- Responsable (electrónico/físico): Titular de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social.
Funciones: Coordinar las actividades para el desarrollo del procedimiento de gestión y seguimiento de peticiones ciudadanas y la operación del SIGC.
Obligaciones: Dirigir las acciones para dar cumplimiento a las normativas de atención.

- Encargado (electrónico): Soporte Administrativo de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social (Personal operativo).
Funciones: Supervisar las actividades para la correcta operación del SIGC.
Obligaciones: Coordinar la operación y dar seguimiento a las inconsistencias del SIGC.





- Encargado (físico): Soporte Administrativo de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social (Personal operativo).
Funciones: Supervisar las actividades para el correcto funcionamiento del archivo de trámite.
Obligaciones: Coordinar el proceso de elaboración de expedientes y monitoreo de los mismos.

- Usuarios (electrónico y físico), Soportes Administrativos (Personal operativo).

- Apoyos Administrativos (Personal operativo).

Funciones: Registrar información de datos personales en el SIGC.
Obligaciones: Usuario con contraseña personal e intransferible que deberá realizar actividades del proceso de atención de peticiones ciudadanas, captura de datos en el SIGC para generar un expediente electrónico, seguimiento y/o aclaraciones desde expediente físico.

- Apoyo técnico (Electrónico), Soporte Administrativo de la Subdirección de Administración de Desarrollo de Personal e Informática.
Funciones: Administrador del servidor del SIGC.
Obligaciones: Apoyo al encargado en el soporte técnico del SIGC.

III. EL ANÁLISIS DE RIESGOS

El análisis de riesgos se realiza de conformidad con lo establecido en los artículos 27, fracción IV, 29, fracción III de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 60 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, que al pie de la letra señalan que:

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

[…]

Artículo 27. *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*

[…]

IV. *Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*

[…]





Artículo 29. *El responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*

[…]

III. *El análisis de riesgos;*

[…]

LINEAMIENTOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR PÚBLICO

[…]

Artículo 60. *Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:*

I. *Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;*

II. *El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;*

III. *El valor y exposición de los activos involucrados en el tratamiento de los datos personales;*

IV. *Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y*

V. *Los factores previstos en el artículo 32 de la Ley General.*

[…]

Para mayor referencia, consultar lo descrito en el anexo de Activos de TI y riesgos de acuerdo a los lineamientos y normatividad previstos por la Ley. (Anexo 2) Dicha información no puede ser proporcionada al público en general, toda vez que se trata de información susceptible de ser clasificada de conformidad con la normativa aplicable.

IV. EL ANÁLISIS DE BRECHA

El análisis de brecha se realiza de conformidad con lo establecido en los artículos 27, fracción V, 29, fracción IV de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 61 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público., que al pie de la letra señalan que:

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

[…]

Artículo 27. *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*

[…]

V. *Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*





[…]

Artículo 29. *El responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*

[…]

IV. *El análisis de brecha;*

[…]

LINEAMIENTOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR PÚBLICO

[…]

Artículo 61. *Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:*

I. *Las medidas de seguridad existentes y efectivas;*

II. *Las medidas de seguridad faltantes, y*

III. *La existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.*

[…]

Para mayor referencia, consultar lo descrito en el anexo de Activos de TI y riesgos de acuerdo a los lineamientos y normatividad previstos por la Ley. (Anexo 2) Dicha información no puede ser proporcionada al público en general, toda vez que se trata de información susceptible de ser clasificada de conformidad con la normativa aplicable.

V. PLAN DE TRABAJO

El plan de trabajo se realiza de conformidad con lo establecido en los artículos 27, fracción VI, 29, fracción V y 31 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como el artículo 62 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Para mayor referencia, consultar lo descrito en el anexo de Activos de TI y riesgos de acuerdo a los lineamientos y normatividad previstos por la Ley. (Anexo 2) Dicha información no puede ser proporcionada al público en general, toda vez que se trata de información susceptible de ser clasificada de conformidad con la normativa aplicable.

VI. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Para evaluar y medir los resultados de la implementación de las medidas de seguridad, se acata lo dispuesto en los artículos 24, fracciones IV y V, 27, fracción VII, así como el artículo 29 fracción VI, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 49 y 63 de los Lineamientos Generales de Protección de Datos Personales del Sector Público, que se reproducen a continuación:





LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

Artículo 24. *Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:*

[…]

IV. *Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;*

V. *Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;*

[…]

Artículo 27. *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*

[…]

VII. *Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y*

[…]

Artículo 29. *El responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*

[…]

VI. *Los mecanismos de monitoreo y revisión de las medidas de seguridad, y*

[…]

LINEAMIENTOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR PÚBLICO

Artículo 49. *Con relación al artículo 30, fracciones IV y V de la Ley General, por regla general, el responsable deberá revisar las políticas y programas de seguridad y el sistema de supervisión y vigilancia implementado, al menos, cada dos años, salvo que realice modificaciones sustanciales a los tratamientos de datos personales que lleve a cabo y, en consecuencia, amerite una actualización previa al plazo establecido en el presente artículo.*

[…]

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

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

I. *Los nuevos activos que se incluyan en la gestión de riesgos;*





II. *Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;*

III. *Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;*

IV. *La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;*

V. *Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;*

VI. *El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y*

VII. *Los incidentes y vulneraciones de seguridad ocurridas.*

[…]

En cumplimiento a la normatividad citada, la Mtra. Verónica Pinal González, Titular de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social evaluará, de manera semestral, los resultados de las acciones implementadas para garantizar la protección y tratamiento de los datos personales, esto, valorando las nuevas amenazas que puedan explotar sus vulnerabilidades, detectando nuevas vulnerabilidades en el tratamiento de los datos personales y los factores de riesgo, los incidentes y vulneraciones ocurridas, para posteriormente evaluar si las medidas de seguridad están operando y, de ser así, si realmente están mitigando los factores de riesgo.

Lo anterior, se realizará a través de los análisis de riesgo y de brecha, así como a través del Diagnóstico de Monitoreo y Revisión de Medidas de Seguridad, que contemplan las medidas de seguridad existentes, los activos involucrados, la posibilidad de identificar las nuevas posibles amenazas, incidentes y/o vulneraciones a los datos personales, así como los que ya ocurrieron, evaluando su impacto y posibles consecuencias.

Posteriormente, se realizará un informe de los resultados obtenidos, con la finalidad de desarrollar un plan de trabajo para la implementación de las medidas de seguridad necesarias, que contemplará las siguientes acciones:

- Revisión y, en su caso, actualización del documento de seguridad, en sus apartados:

    - Inventario de datos personales y de los sistemas de tratamiento
    - Funciones y obligaciones de las personas servidoras públicas usuarias
    - Análisis de riesgo
    - Análisis de brecha
    - Medidas de seguridad





- Reforzamiento de conocimientos, a través de la capacitación y asesoría con la Unidad de Transparencia.

- Mesas de trabajo permanentes con los usuarios del tratamiento de datos personales para resolver dudas, plantear problemáticas y hacer recomendaciones relacionadas con el tratamiento y manejo de los datos.

Una vez realizado el informe y después de haber identificado nuevas posibles amenazas, vulneraciones o incidentes referentes al tratamiento de los datos personales, el documento de seguridad se puede actualizar de conformidad con lo establecido en el artículo 30, fracción II de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que al pie de la letra señala que:

> ***Artículo 30.*** *El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:*
>
> *[…]*
>
> ***II.*** *Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;*
>
> *[…]*

El formato que se llena dentro de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social para realizar el monitoreo y revisión de las medidas de seguridad es el siguiente:

1. Con el objeto de impedir que, cualquier tratamiento de datos personales contravenga las disposiciones aplicables a la materia, ¿se establecieron las siguientes medidas de seguridad para la protección de los datos personales?	**CUMPLE**
Medidas de seguridad de carácter administrativo	
Implementación del programa general de capacitación	SI
Sensibilización en materia de datos personales	SI
Medidas de seguridad de carácter físico	
Resguardo obligatorio del expediente bajo llave en archiveros	SI
Control de acceso restringido mediante bitácora	SI
Medidas de seguridad de carácter técnico	
Implementación de credenciales electrónicas exclusivas para el resguardo y acceso a los archivos electrónicos	SI
Política obligatoria de cambio de contraseñas de acceso cada seis meses	SI





2. Para establecer 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, ¿se han adoptado las siguientes medidas de seguridad?	CUMPLE
El riesgo inherente a los datos personales tratados;	SI
La sensibilidad de los datos personales tratados	SI
El desarrollo tecnológico	SI
Las posibles consecuencias de una vulneración para los titulares	SI
Las transferencias de datos personales que se realicen	SI
El número de titulares	SI
Las vulneraciones previas ocurridas en los sistemas de tratamiento	No hay indicios de vulneraciones
El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.	SI

3. En el diseño e implementación de las políticas internas para la gestión y el tratamiento de los datos personales, ¿se incluyó, al menos, lo siguiente?	CUMPLE
Todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.	SI
Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen.	SI
Las sanciones en caso de incumplimiento.	SI
La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados.	SI
El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales.	SI
El proceso general de atención de los derechos ARCO.	SI





4. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, ¿se realizaron, al menos, las siguientes actividades interrelacionadas?	CUMPLE
Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.	SI
Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.	SI
Elaborar un inventario de datos personales y de los sistemas de tratamiento.	SI
Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.	SI
Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;	SI
Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.	SI
Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.	SI
Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.	SI

5. En la elaboración del documento de seguridad, ¿se encuentran los siguientes puntos?	CUMPLE
El inventario de datos personales y de los sistemas de tratamiento.	SI
Las funciones y obligaciones de las personas que traten datos personales.	SI
El Análisis de riesgos.	SI
El análisis de brecha.	SI
El plan de trabajo.	SI
Los mecanismos de monitoreo y revisión de las medidas de seguridad.	SI
El programa general de capacitación.	SI

6. Respecto a la elaboración del inventario ¿se consideraron, al menos, los siguientes elementos?	CUMPLE
El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales.	SI
Las finalidades de cada tratamiento de datos personales.	SI
El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no.	SI





El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales.	SI
La lista de servidores públicos que tienen acceso a los sistemas de tratamiento.	SI
En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable.	SI
En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.	SI
¿El inventario cuenta información básica de cada uno de los tratamientos de datos personales?	SI

6.1 En la elaboración del inventario, ¿se consideró el ciclo de vida de los datos personales, conforme a lo siguiente?	**CUMPLE**
La obtención de los datos personales.	SI
El almacenamiento de los datos personales.	SI
El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin.	SI
La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen.	SI
El bloqueo de los datos personales, en su caso.	SI
La cancelación, supresión o destrucción de los datos personales.	SI

6.2 En la elaboración del inventario ¿se identificaron riesgos inherentes a los siguientes puntos?	**CUMPLE**
Se contempló el ciclo de vida y los activos involucrados en el tratamiento de los datos personales	SI
Hardware	SI
Software.	SI
Personal.	SI
Cualquier otro recurso humano o material que resulte pertinente considerar.	SI

7. Por lo que respecta a las funciones y obligaciones de las personas que traten datos personales, ¿se tomaron en cuenta los siguientes elementos?	**CUMPLE**
Establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema de gestión implementado.	SI
Establecer mecanismos para asegurar que todas las personas involucradas en el tratamiento de datos personales, conozcan sus funciones para el cumplimiento de los objetivos del sistema de gestión, así como las consecuencias de su incumplimiento.	SI





8 Al realizar el análisis de riesgos de los datos personales tratados, ¿se consideró lo siguiente?	CUMPLE
Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.	SI
El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.	SI
El valor y exposición de los activos involucrados en el tratamiento de los datos personales.	SI
Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.	SI
Los factores previstos en el numeral 2, del presente listado.	SI

8.1 Con la finalidad de establecer y vigilar los mecanismos que permitan la administración de la seguridad de la información de la Institución, así como disminuir el impacto de eventos adversos, ¿se consideró lo siguiente?	CUMPLE
El establecimiento, operación y mantenimiento de un modelo de gobierno de seguridad de la información	SI
La identificación de infraestructuras críticas y activos claves de la Institución y la elaboración del catálogo respectivo	SI
Establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar atender y monitorear los riesgos.	SI
Establecer un Sistema de Gestión de la Seguridad de la Información que proteja los activos de información de la Institución, con la finalidad de preservar su confidencialidad, integridad y disponibilidad.	SI
Establecer mecanismos para la respuesta inmediata a incidentes a la seguridad de la información.	SI
Vigilar los mecanismos establecidos y el desempeño del Sistema de Gestión de la Seguridad de la Información a fin de prever desviaciones y mantener una mejora continúa	SI
Fomentar una cultura de seguridad de la información en la institución.	SI

8.2 Con el propósito de identificar, clasificar y priorizar los riesgos para evaluar su impacto sobre los procesos y los servicios de la Institución, ¿se efectuaron las siguientes acciones?	CUMPLE
La definición de estrategias, metodologías y herramientas que se usarán para administrar los riesgos.	SI
La integración del marco normativo que resulte aplicable a los riesgos identificados.	SI
El establecimiento de las reglas para medir la efectividad de los controles en la gestión de los riesgos.	SI





La definición de la forma y periodicidad con las que se informará sobre los riesgos a los que se encuentran expuestos los procesos y servicios que se utilizan.	SI
La definición de consideraciones sobre riesgos de TIC y seguridad a la información que coadyuven en la toma de decisiones estratégicas de la Institución.	SI

9. Para la realización del análisis de brecha, ¿el responsable consideró lo siguiente?	**CUMPLE**
Las medidas de seguridad existentes y efectivas.	SI
Las medidas de seguridad faltantes.	SI
La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.	SI
Realizar pruebas de penetración	SI

10. ¿El responsable elaboró un plan de trabajo, en el que se definieron las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, tomando en consideración lo siguiente?	**CUMPLE**
Los recursos designados las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.	SI
El personal interno y externo en su organización	SI
Las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.	SI

11. Con la finalidad verificar el cumplimiento de los objetivos propuestos en materia de seguridad y tratamiento de los datos personales, ¿se monitorea continuamente lo siguiente?	**CUMPLE**
Los nuevos activos que se incluyan en la gestión de riesgos.	SI
Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras.	SI
Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas.	SI
La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.	SI
Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir.	SI
El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.	SI
Los incidentes y vulneraciones de seguridad ocurridas.	SI





12. ¿Con el propósito de capacitar a los involucrados internos y externos, se diseñaron e implementaron programas a corto, mediano y largo plazo, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos, tomando en cuenta lo siguiente?	CUMPLE
Los requerimientos y actualizaciones del sistema de gestión.	SI
La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos.	SI
Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales.	SI
Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.	SI

13. ¿Se actualiza el documento de seguridad cuando ocurren los siguientes eventos?	CUMPLE
Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.	SI
Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.	SI
Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.	SI
Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.	SI

14. Adicional a las que señalen las leyes respectivas y la normatividad aplicable, ¿se consideran como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, las siguientes?	CUMPLE
La pérdida o destrucción no autorizada;	SI
El robo, extravío o copia no autorizada	SI
El uso, acceso o tratamiento no autorizado, o	SI
El daño, la alteración o modificación no autorizada.	SI
Alguna otra	SI

15. En la bitácora de las vulneraciones a la seguridad, ¿se describe la siguiente información?	CUMPLE
Fecha en la que ocurrió	SI
Motivo de ésta	SI
Acciones correctivas implementadas de forma inmediata y definitiva	SI





16. En caso de alguna vulneración a los datos personales, ¿se proporciona un informe al titular, señalando lo siguiente?	CUMPLE
La naturaleza del incidente;	SI
Los datos personales comprometidos;	SI
Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;	SI
Las acciones correctivas realizadas de forma inmediata, y	SI
Los medios donde puede obtener más información al respecto.	SI

VII. PROGRAMA GENERAL DE CAPACITACIÓN

En cumplimiento con lo establecido en los artículos 24, fracción III, 27, fracción VIII, 29, fracción VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como los artículos 48 y 64 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, los cuales señalan que:

LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

Artículo 24. *Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:*
[…]
III. *Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;*
[…]
Artículo 27. *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
[…]
VIII. *Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.*
[…]
Artículo 29. *El responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*
[…]
VII. *El programa general de capacitación*
[…]

LINEAMIENTOS GENERALES DE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR PÚBLICO

Artículo 48. *Con relación al artículo 30, fracción III de la Ley General, el responsable deberá establecer anualmente un programa de capacitación y actualización en materia de protección de datos personales dirigido a su personal y a encargados, el cual deberá ser aprobado, coordinado y supervisado por su Comité de Transparencia.*
[…]
Artículo 64. *Para el cumplimiento de lo previsto en el artículo 33, fracción VIII de la Ley General, el responsable deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a*





los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de sus puestos.
En el diseño e implementación de los programas de capacitación a que se refiere el párrafo anterior del presente articulo, el responsable deberá tomar en cuenta lo siguiente:
***I.** Los requerimientos y actualizaciones del sistema de gestión;*
***II.** La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;*
***III.** Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y*
***IV.** Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.*
[…]

Por lo anterior, y derivado de las funciones de captación de datos personales que realiza la Secretaría de Salud, la Unidad Coordinadora de Vinculación y Participación Social a través de la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social, determina la necesidad de diseñar e implementar cursos de capacitación y sensibilización en materia de protección de datos personales dirigidas al personal que realiza el tratamiento de los datos, así como también cursos sobre las medidas de seguridad para el tratamiento de datos personales físicos y electrónicos, y de apoyo para la elaboración y actualización del documento de seguridad y avisos de privacidad, de acuerdo con el programa general de capacitación que se señala a continuación:

Las personas servidoras públicas que traten datos personales deberán contar con capacitación constante y conforme al desarrollo de sus habilidades específicas para el puesto que desempeña, por medio de programas de capacitación y actualización para las personas servidoras públicas en materia de protección de datos personales la capacitación se realizará en coordinación con la Autoridad Garante, conforme a los artículos 81, fracción XXIII, 83, fracción XIII y 84 de la LGPDPPSO.

Programa general de capacitación				
Módulo	**Objetivo**	**Duración**	**Imparte**	**Modalidad**
Curso 1.- Concientización de la protección de los datos personales				
1) Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados	Familiarizarse con las disposiciones establecidas en la ley, así como la importancia de la protección a los datos personales	1 semana	Unidad Coordinadora de Vinculación y Participación Social	Presencial





2) Datos personales y datos personales sensibles	Establecer y entender la definición de ambos conceptos, así como cuáles son las principales diferencias entre ellos	1 semana	Unidad Coordinadora de Vinculación y Participación Social	Presencial
3) Tratamiento de los datos personales	Que el personal conozca cuales son los medios por los que se obtienen y resguardan los datos personales, así como el debido proceso por el que se deben de tratar	1 semana	Unidad Coordinadora de Vinculación y Participación Social	Presencial
Curso 2.- Tratamiento de datos personales electrónicos				
1) Medios electrónicos de recabación y resguardo	Identificar los medios electrónicos por los que se recaban y resguardan los datos personales dentro de la Dirección	2 semanas	Unidad Coordinadora de Vinculación y Participación Social	Presencial
2) Amenazas electrónicas al tratamiento de datos personales	Comprender los riesgos de pérdida, robo o daño a los que son susceptibles los datos personales electrónicos durante su tratamiento	1 mes	Unidad Coordinadora de Vinculación y Participación Social	Presencial
3) Medidas de seguridad para las amenazas electrónicas	Identificar y proponer soluciones para subsanar posibles amenazas y garantizar la seguridad del tratamiento a los datos personales electrónicos	1 mes	Unidad Coordinadora de Vinculación y Participación Social	Presencial





4) Mecanismos de monitoreo y revisión de las medidas de seguridad	Entender la implementación de revisiones y monitoreo para verificar que las medidas de seguridad estén cumpliendo con su objetivo	1 mes	Unidad Coordinadora de Vinculación y Participación Social	Presencial
Curso 3.- Tratamiento de datos personales físicos				
1) Medios físicos de recabación y resguardo	Identificar los medios físicos por los que se recaban y resguardan los datos personales dentro de la Dirección	1 mes	Unidad Coordinadora de Vinculación y Participación Social	Presencial
2) Amenazas físicas al tratamiento de datos personales	Comprender los riesgos de pérdida, robo o daño a los que son susceptibles los datos personales físicos durante su tratamiento	1 mes	Unidad Coordinadora de Vinculación y Participación Social	Presencial
3) Medidas de seguridad para las amenazas físicas	Identificar y proponer soluciones para subsanar posibles amenazas y garantizar la seguridad del tratamiento a los datos personales físicos	1 mes	Unidad Coordinadora de Vinculación y Participación Social	Presencial
4) Mecanismos de monitoreo y revisión de las medidas de seguridad	Entender la implementación de revisiones y monitoreo para verificar que las medidas de seguridad estén cumpliendo con su objetivo	1 mes	Unidad Coordinadora de Vinculación y Participación Social	Presencial





Curso 4.- Elaboración y actualización del documento de seguridad				
1) Definición, actualización y estructura del documento de seguridad	Que el personal conozca el documento de seguridad a elaborar para el tratamiento de los datos personales, así como su estructura completa	1 semana	Unidad Coordinadora de Vinculación y Participación Social	Presencial
2) Inventario de datos personales y los sistemas de tratamiento	Entender cómo abarcar todos los sistemas de tratamiento de datos personales físicos y electrónicos, así como su obtención, almacenamiento, etc.	1 mes	Unidad Coordinadora de Vinculación y Participación Social	Presencial
3) Funciones y obligaciones de las personas que traten datos personales	Que el personal reconozca que papel cumple cada uno de los usuarios en el tratamiento de los datos personales físicos y electrónicos	1 mes	Unidad Coordinadora de Vinculación y Participación Social	Presencial
4) Análisis de riesgos y de brecha	Que el personal aprenda a valorar los riesgos administrativos, físicos o tecnológicos a los que se someten los datos personales para subsanarlos	1 mes	Unidad Coordinadora de Vinculación y Participación Social	Presencial
5) Plan de trabajo	Que el personal conozca cómo elaborar el plan de trabajo para subsanar los	1 mes	Unidad Coordinadora de Vinculación y Participación Social	Presencial



	posibles riesgos expuestos en el análisis			

Adicional a lo establecido en el programa general de capacitación, que comprende una duración de un año, también se implementan las siguientes acciones en aras de robustecer los mecanismos de protección de datos personales en esta Dirección de Gestión de Peticiones Ciudadanas y Promoción Social:

- Acreditación de los usuarios al concluir los cursos contemplados en el programa general de capacitación, así como de aquellos que imparta Transparencia para el Pueblo y Secretaría Anticorrupción y Buen Gobierno, en materia de transparencia, acceso a la información pública y protección de datos personales para la capacitación y mejora continua del personal.

- Establecer y promover los principios y deberes en materia de protección de datos personales.

- Impartir pláticas y sostener reuniones de trabajo en coordinación con la Unidad de Transparencia para coadyuvar en las acciones relativas a la protección de datos personales.

- Impartir pláticas y sostener reuniones de trabajo en coordinación con la Dirección General de Tecnologías de la Información, con la finalidad de instruir al personal en el correcto uso y funcionamiento de equipos de cómputo y entornos digitales.

ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente documento de seguridad se actualizará siempre y cuando se suponga uno de los eventos previstos en el artículo 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el cual al pie de la letra señala que:

[…]

Artículo 30. *El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:*

I. *Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;*

II. *Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;*

III. *Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y*

IV. *Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.*



[...]

En caso de que exista una actualización de este documento de seguridad se hará de conocimiento a las personas titulares a través de la página Web de la Secretaría de Salud http://portal.salud.gob.mx/sites/transparencia/transparencia/proteccion_datos/privacidad_1.html, o de manera presencial en la Dirección de Gestión de Peticiones Ciudadanas y Promoción Social.

