Unidad de Transparencia
Folio: **210421524000759**
Fecha: 31/10/2024

C. Julieta del Mazo F.:

En atención a su solicitud, relativa a conocer:
"Se me informe qué políticas en materia de protección de datos personales han diseñado y/o implementado.
Se me entregue el documento de seguridad.
¿Qué medidas de seguridad han adoptado para mantener exactos, completos, correcto y actualizados los datos personales?
¿Qué procedimientos han establecidos para la conservación y en su caso, bloqueo y supresión de los datos personales?
Qué procedimientos han implementado y/o desarrollado para recibir y responder dudas y quejas de los titulares de los datos personales y en que consiste?
Qué mecanismos han utilizados y/o aplicados para cumplir con los plazos fijados para la supresión de los datos personales?
En los años 2010 a la fecha que mecanismos y/o desarrollado han aplicado para la revisión periódica sobre la necesidad de conservar los datos personales y cuáles son.?
Qué códigos de buenas prácticas y/o modelo en materia de protección de datos personales han implementado y/o realizado y/o elaborado ect.
Qué programas y/o políticas de protección de datos personales han implementado y/o realizado y/o elaborado ect.
Solicito su programa de capacitación en materia de datos personales han aplicado en su institución y/o dependencia de los años 2023 y 2024.
Qué programas y/o políticas de seguridad de datos personales han implementado en su institución y/o dependencia de los años 2023 y 2024 y cuáles son?
Qué programas y/o servicios y/o sistemas y/o plataformas informáticas han realizado y/o implementado y/o diseñado para el tratamiento de los datos personales?
Qué medidas de seguridad han implementado para mantener la seguridad para la protección de los datos personales que permitan protegerlo contra daño, y/o pérdida y/o alteración y/o destrucción para garantizar su confidencialidad, integridad y disponibilidad.
Se me entregué en copia escaneada de la bitácora de las vulneraciones de seguridad que han tenido sobre los tratamientos de los datos personales.
Cuántos casos de vulneración han reportado al órgano garante sobre la vulneraciones de los datos personales en los años de 2010 a la fecha.
Qué mecanismos y/o controles han implementado y/o realizado sobre aquellas personas y/o servidores públicos que intervengan para garantizar y guardar la confidencialidad sobre los datos personales que utilizan en sus tratamientos de los datos personales.
Cuántas personales y/o servidores públicos manejan datos personales se me informen por su nombre de los servidores públicos, área de adscripción y el cargo.
Cuántas solicitudes de derechos ARCOP han recibido desde de los años 2010 a la fecha, además se informe por mes cuántas han recibido y esas cuantas ha sido de acceso, rectificación, cancelación,

oposición y de portabilidad, y cuántas son hombres y mujeres y cuales se han declarado la inexistencia de los datos personales.
Copia escaneada del nombramiento de su oficial de protección de datos personales.
Solicito el programa de capacitación del comité de transparencia y/o unidad de transparencia y/o oficial de protección de datos personales en materia de protección de datos personales de los años 2023 y 2024.
Se me informe sobre los procedimientos que han implementado y/o realizado para la eficiencia de la gestión de las solicitudes de derechos ARCOP y que área lo realizó.
Cuántas transferencias han realizado en materia de datos personales en este año 2024 y que áreas administrativas lo han realizado
Cuentan con el Programa Integral de Gestión de Datos, en caso de contar con dicho programa se me proporcione.
Qué mecanismos han implementado y/o realizado para asegurar que los datos personales se entreguen solo a sus titulares y/o representantes.
Cuantos servidores públicos integran su unidad de transparencia.
Cuántas auditorías en materia de datos personales le han solicitado al órgano garante desde el 2010 a la fecha.
Se me informe si han remitido el informe semestral referente al número de requerimientos de localización geográfica en tiempo real y de registro de datos realizados, así como el número de registros de datos de comunicaciones cancelados y suprimidos de manera segura, una vez cumplido el fin para el cual fueron solicitados, de los años 2010 a la fecha.
Referente al informe antes solicitado se me entregue el link donde pueda consultar la información estadística de dicho informe.
Cuántas denuncias en materia de datos personales han recibido desde el años 2010 a la fecha.
Se me explique cuáles son las medidas que aplican para uno de los principios incorporados en la LGPDPPSO, para garantizar el tratamiento de los datos personales.
Qué sujetos obligados han presentado su evaluación de impacto en la protección de datos personales en los años 2020 a la fecha.
Cuantas recomendaciones no vinculantes han emitido sobre el contenido de la evaluación de impacto de los años 2020 a la fecha.
Cuántas denuncias en materia de obligaciones de transparencia han recibido desde el año 2020 a la fecha y el sentido de la resolución.
Qué programa y/o acciones han implementado en materia de gobierno abierto."

De acuerdo en lo dispuesto en el artículo 6 apartado A, de la Constitución Política de los Estados Unidos Mexicanos; 4, 6, 129, 132 y 133 de la Ley General de Transparencia y Acceso a la Información Pública; 6, 8, 11, 22, 142, 150, 154, 156 fracción IV de la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla; artículos 186 y 187 del Reglamento de la Ley Orgánica de la Fiscalía General del Estado; normatividad que otorga facultades y determina el actuar de la Unidad de Transparencia, para dar trámite y respuesta a las solicitudes de acceso a la información que se presenten ante la Fiscalía General del Estado.

Para tal efecto, el derecho de acceso a la información comprende el solicitar, investigar, difundir, buscar y recibir información; y determinar que toda la información generada, adquirida, obtenida, transformada o en posesión de los sujetos obligados se considera información pública, accesible a cualquier persona en los términos y condiciones que establece la Ley y demás normatividad aplicable; para ello, los sujetos obligados deberán otorgar acceso a los documentos que se encuentren en sus archivos o que estén obligados a documentar de acuerdo con sus facultades, competencias o funciones en el formato en que el solicitante manifieste, de entre aquellos formatos existentes, conforme a las características físicas de la información o del lugar donde se encuentre así lo permita, privilegiando en todo momento que la entrega sea en los formatos solicitados.

De lo anterior, hacemos de su conocimiento la siguiente información tal y como obran en los archivos de esta Fiscalía:

Se me informe qué políticas en materia de protección de datos personales han diseñado y/o implementado.
Respuesta: Se emitieron: "Lineamientos para la Protección de Datos Personales de Mujeres Víctimas de Delito", "Lineamientos L/011/2021 para el Cumplimiento de las obligaciones de Transparencia, Acceso a la Información y Protección de Datos Personales", "Documento de Seguridad para la Protección de Datos Personales"

Se me entregue el documento de seguridad.
Respuesta: Se adjunta el documento de seguridad para la protección de datos personales 2024.

¿Qué medidas de seguridad han adoptado para mantener exactos, completos, correcto y actualizados los datos personales?
Respuesta:

Acciones	Temporalidad	Responsable	Descripción
Medidas cotidianas de protección de datos personales			
Gestión de datos			

www.fiscalia.puebla.gob.mx /fiscaliapuebla @FiscaliaPuebla
Blvd. Héroes del 5 de Mayo y 31 Oriente, col. Ladrillera de Benítez
C.P. 72530, Puebla, Pue. (222) 211 79 00 Ext. 4019 y 4050

personales	Permanente	Usuario de los datos personales	Se respetarán las medidas implementadas para el mantenimiento de los diferentes controles establecidos para salvaguardar los datos personales relacionados durante su tratamiento
Prevención del mal uso de activos informáticos	Permanente	Coordinación General de Estadística y Sistemas de Información	Se deben tener mecanismos contra el uso de activos para propósitos no autorizados, como son los sistemas electrónicos, la utilización de bloqueos en caso de que usuarios no autorizados traten de acceder a módulos que no tienen permitido.
Cumplimiento legal			
Identificación de legislación aplicable	Al momento de iniciar el tratamiento de datos personales	Usuario de los datos personales con auxilio de ser necesario de la Coordinación General de Asuntos Jurídicos	Se identificarán los deberes y responsabilidades para cumplir con los requerimientos legales relacionados con la protección de datos personales.
Actualización de registro de usuarios	Cada que se lleven a cabo modificaciones	Encargado del registro de cada Unidad Administrativa	Se deben mantener actualizados los registros de los usuarios de datos personales.

Acciones	Temporalidad	Responsable	Descripción
Comunicación permanente al momento de llevar	Al momento de que se lleve a cabo la	Los servidores públicos que realicen la	Cuando se lleva a cabo la transferencia de datos personales entre sujetos obligados o entre

www.fiscalia.puebla.gob.mx /fiscaliapuebla @FiscaliaPuebla
Blvd. Héroes del 5 de Mayo y 31 Oriente, col. Ladrillera de Benítez
C.P. 72530, Puebla, Pue. (222) 211 79 00 Ext. 4019 y 4050

a cabo transferencia de datos personales	transferencia de datos personales	transferencia	servidores públicos de la Fiscalía General, se realizará el apercibimiento en cuanto al trato que se le deberá dar a los mismos, en los términos de la legislación vigente en la materia.
Recomendaciones en materia de seguridad de la información	Al momento de identificarlas	Personal de la Unidad de Transparencia	Cuando sea adecuado, obtener el consejo y recomendaciones de un especialista en protección de datos y seguridad de la información.
Acompañamiento	Al momento de que acontezca una contingencia	Personal adscrito a la Unidad de Transparencia y a la Coordinación General de Asuntos Jurídicos	Se llevará a cabo el acompañamiento y asesoría del personal adscrito a la Unidad de Transparencia y a la Coordinación General de Asuntos Jurídicos al momento de llevar a cabo las acciones apropiadas en caso de un incidente o vulneración de seguridad.
Estructura organizacional			
Designación de deberes en seguridad y protección de datos personales	Al momento de identificarlas	Titulares de las Unidades Administrativas	Se deben designar deberes y obligaciones respecto a los servidores públicos que intervengan en el uso y protección de datos personales.
Contratos con proveedores	Permanente	Área contratante	En la elaboración de los contratos con proveedores, revisar las cláusulas referentes a los requerimientos de seguridad y de tratamiento de datos personales para verificar su correspondencia con los requerimientos de la Fiscalía General.
Seguridad del personal			

www.fiscalia.puebla.gob.mx /fiscaliapuebla @FiscaliaPuebla
Blvd. Héroes del 5 de Mayo y 31 Oriente, col. Ladrillera de Benítez
C.P. 72530, Puebla, Pue. (222) 211 79 00 Ext. 4019 y 4050

Capacitación	Anualmente	Unidad de Transparencia	Los servidores públicos de la Unidad de Transparencia privilegiarán la asesoría en materia de datos personales para los servidores públicos de la Fiscalía General, incluyéndolos en su plan anual de capacitación.
Resguardo de la documentación	Permanente	Usuario de los datos personales	Cualquier documento o activo de información crítico debe estar resguardado, fuera de la vista, cuando éste no sea atendido.

¿Qué procedimientos han establecidos para la conservación y en su caso, bloqueo y supresión de los datos personales?
Respuesta: Se adjunta el documento que contiene el Procedimiento para la Conservación, Modificación y Supresión de Datos Personales de la Fiscalía General del Estado de Puebla

¿Qué procedimientos han implementado y/o desarrollado para recibir y responder dudas y quejas de los titulares de los datos personales y en qué consiste?
Respuesta: De conformidad con el artículo 116 de Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla; y artículo 187 del Reglamento de la Ley Orgánica de la Fiscalía General del Estado; el personal adscrito a la Unidad de Transparencia tiene la atribución de asesorar, auxiliar y orientar al Titular o, en su caso, a su representante legal que lo requiera con relación al ejercicio del derecho a la protección de Datos Personales. La Unidad de Transparencia cuanta con los siguientes medios de comunicación para tal efecto:

Dirección: Boulevard Héroes del 5 de mayo y 31 oriente, colonia Ladrillera de Benítez, Puebla, Puebla. C.P. 72539.
Teléfono: (222) 211 79 00 ext. 4019.
Correo electrónico: unidad.transparencia@fiscalia.puebla.gob.mx

¿Qué mecanismos han utilizados y/o aplicados para cumplir con los plazos fijados para la supresión de los datos personales?
Respuesta: De conformidad con el Procedimiento para la Conservación, Modificación y Supresión de Datos Personales de la Fiscalía General del Estado de Puebla

¿En los años 2010 a la fecha que mecanismos y/o desarrollado han aplicado para la revisión periódica sobre la necesidad de conservar los datos personales y cuáles son?

Respuesta: De conformidad con el Procedimiento para la Conservación, Modificación y Supresión de Datos Personales de la Fiscalía General del Estado de Puebla

Qué códigos de buenas prácticas y/o modelo en materia de protección de datos personales han implementado y/o realizado y/o elaborado etc.
Respuesta: Los "Lineamientos para la Protección de Datos Personales de Mujeres Víctimas de Delito", "Lineamientos L/011/2021 para el Cumplimiento de las obligaciones de Transparencia, Acceso a la Información y Protección de Datos Personales", "Documento de Seguridad para la Protección de Datos Personales"

Qué programas y/o políticas de protección de datos personales han implementado y/o realizado y/o elaborado etc.
Respuesta: Los "Lineamientos para la Protección de Datos Personales de Mujeres Víctimas de Delito", "Lineamientos L/011/2021 para el Cumplimiento de las obligaciones de Transparencia, Acceso a la Información y Protección de Datos Personales", "Documento de Seguridad para la Protección de Datos Personales"

Solicito su programa de capacitación en materia de datos personales han aplicado en su institución y/o dependencia de los años 2023 y 2024.
Respuesta: Los programas de capacitación se encuentran en el "Documento de Seguridad para la Protección de Datos Personales 2023" y "Documento de Seguridad para la Protección de Datos Personales2024", mismos que se adjuntan.

¿Qué programas y/o políticas de seguridad de datos personales han implementado en su institución y/o dependencia de los años 2023 y 2024 y cuáles son?
Respuesta: "Documento de Seguridad para la Protección de Datos Personales 2023" y "Documento de Seguridad para la Protección de Datos Personales2024", mismos que se adjuntan.

¿Qué programas y/o servicios y/o sistemas y/o plataformas informáticas han realizado y/o implementado y/o diseñado para el tratamiento de los datos personales?
Respuesta: Se cuenta con cero registros de la información solicitada.

Qué medidas de seguridad han implementado para mantener la seguridad para la protección de los datos personales que permitan protegerlo contra daño, y/o pérdida y/o alteración y/o destrucción para garantizar su confidencialidad, integridad y disponibilidad.
Respuesta: "Documento de Seguridad para la Protección de Datos Personales 2023" y "Documento de Seguridad para la Protección de Datos Personales2024", mismos que se adjuntan.

Se me entregué en copia escaneada de la bitácora de las vulneraciones de seguridad que han tenido sobre los tratamientos de los datos personales.
Respuesta: Se cuenta con cero registros vulneraciones en el tratamiento de datos personales.

Cuántos casos de vulneración han reportado al órgano garante sobre las vulneraciones de los datos personales en los años de 2010 a la fecha.
Respuesta: Se cuenta con cero registros vulneraciones en el tratamiento de datos personales.

Qué mecanismos y/o controles han implementado y/o realizado sobre aquellas personas y/o servidores públicos que intervengan para garantizar y guardar la confidencialidad sobre los datos personales que utilizan en sus tratamientos de los datos personales.
Respuesta: "Documento de Seguridad para la Protección de Datos Personales 2023" y "Documento de Seguridad para la Protección de Datos Personales2024", mismo que se adjuntan.

Cuántas personales y/o servidores públicos manejan datos personales se me informen por su nombre de los servidores públicos, área de adscripción y el cargo.
Respuesta: La información se puede consultar en el directorio de servidores públicos, en el siguiente enlace:

PORTAL DE TRANSPARENCIA DE LA FISCALÍA GENERAL DEL ESTADO
http://www.fiscalia.puebla.gob.mx -- > Transparencia -- > Obligaciones de Transparencia -- > Artículo 77 -- > Fracción VII -- > Directorio ---> Donde podrá consultar la información relativa a los servidores públicos, adscripción y cargo.

En caso de presentar alguna dificultad para la descarga de los documentos aquí señalados, podrá comunicarse a esta Unidad de Transparencia, a los siguientes datos de contacto, para recibir una mejor orientación:

Unidad de Transparencia
Boulevard Héroes del 5 de mayo y 31 oriente, colonia Ladrillera de Benítez, Puebla, Puebla. C.P. 72539.
Teléfono: (222) 211 79 00 ext. 4019.
Correo electrónico: unidad.transparencia@fiscalia.puebla.gob.mx

Cuántas solicitudes de derechos ARCOP han recibido desde de los años 2010 a la fecha, además se informe por mes cuántas han recibido y esas cuantas ha sido de acceso, rectificación, cancelación, oposición y de portabilidad, y cuántas son hombres y mujeres y cuales se han declarado la inexistencia de los datos personales.
Respuesta:

AÑO /MES	2010	2011	2012	2013	2014	2015	2016
ENERO	0	0	0	0	0	0	0
FEBRERO	0	0	0	0	0	0	0

MARZO	0	0	0	0	0	0	0
ABRIL	0	0	0	0	0	0	0
MAYO	0	0	0	0	0	0	0
JUNIO	0	0	0	0	0	0	0
JULIO	0	0	0	0	0	0	0
AGOSTO	0	0	0	0	0	0	0
SEPTIEMBRE	0	0	0	0	0	0	0
OCTUBRE	0	0	0	0	0	0	0
NOVIEMBRE	0	0	0	0	0	0	0
DICIEMBRE	0	0	0	0	0	0	0
TOTAL	**0**	**0**	**0**	**0**	**0**	**0**	**0**

AÑO /MES	2017	2018	2019	2020	2021	2022	2023	2024
ENERO	0	0	0	0	0	0	0	0
FEBRERO	0	1	0	0	0	2	1	0
MARZO	0	1	0	0	0	0	0	1
ABRIL	0	0	0	0	0	2	2	0
MAYO	0	0	0	1	0	6	1	1
JUNIO	0	0	0	0	0	0	2	0
JULIO	0	0	0	0	0	0	0	3
AGOSTO	0	0	0	1	0	0	1	1
SEPTIEMBRE	0	0	0	0	1	1	0	1
OCTUBRE	0	0	0	0	0	1	2	0
NOVIEMBRE	0	0	0	0	0	2	4	0
DICIEMBRE	0	0	0	0	0	0	1	0
TOTAL	**0**	**2**	**0**	**2**	**1**	**14**	**14**	**7**

TIPO DE SOLICITUD	ACCESO	RECTIFICACIÓN	CANCELACIÓN	OPOSICIÓN	PORTABILIDAD
2018	0	0	2	0	-
2019	0	0	0	0	-
2020	2	0	0	0	-
2021	1	0	0	0	-
2022	11	1	1	1	-

2023	14				-
ENE. A OCT. 2024	7				-
TOTAL	**35**	**1**	**3**	**1**	**-**

SEXO DE LOS SOLICITANTES	**MUJERES**	**HOMBRES**
2018		2
2019		
2020	2	
2021		1
2022	2	12
2023	5	9
ENE. A OCT. 2024	3	4
TOTAL	**12**	**28**

Copia escaneada del nombramiento de su oficial de protección de datos personales.
Respuesta: De conformidad con el artículo 187 del Reglamento de la Ley Orgánica de la Fiscalía General del Estado de Puebla, publicado con fecha 16 de junio de 2020; El (la) Titular de la Unidad de Transparencia de esta Fiscalía General del Estado funge como oficial de protección de datos personales en términos de la legislación de protección de datos personales en posesión de sujetos obligados. El citado reglamento podrá ser consultado a través de la siguiente liga electrónica:

PORTAL DE TRANSPARENCIA
http://www.fiscalia.puebla.gob.mx ---> Transparencia ---> Obligaciones de Transparencia ---> Informes --- > Fracción I ---> Normatividad -- > Aquí podrá consultar el marco normativo aplicable a esta Fiscalía, en el que se incluyen leyes, códigos, reglamentos, decretos de creación, manuales administrativos, reglas de operación, criterios, políticas, entre otros.

En caso de presentar alguna dificultad para la descarga de los documentos aquí señalados, podrá comunicarse a esta Unidad de Transparencia, a los siguientes datos de contacto, para recibir una mejor orientación:

UNIDAD DE TRANSPARENCIA

Boulevard Héroes del 5 de mayo y 31 oriente, colonia Ladrillera de Benítez, Puebla, Puebla. C.P. 72539.
Teléfono: 222 211 79 00 Ext. 4019
Correo electrónico: unidad.transparencia@fiscalia.puebla.gob.mx

Solicito el programa de capacitación del comité de transparencia y/o unidad de transparencia y oficial de protección de datos personales en materia de protección de datos personales de los años 2023 y 2024.
Respuesta: Los programas de capacitación se encuentran en el "Documento de Seguridad para la Protección de Datos Personales 2023" y "Documento de Seguridad para la Protección de Datos Personales2024", mismos que se adjuntan.

Se me informe sobre los procedimientos que han implementado y/o realizado para la eficiencia de la gestión de las solicitudes de derechos ARCOP y que área lo realizó.
Respuesta: Lineamientos L/011/2021 para el Cumplimiento de las obligaciones de Transparencia, Acceso a la Información y Protección de Datos Personales.

Cuántas transferencias han realizado en materia de datos personales en este año 2024 y que áreas administrativas lo han realizado
Respuesta: Se tiene cero registros de la información solicitada.

Cuentan con el Programa Integral de Gestión de Datos, en caso de contar con dicho programa se me proporcione.
Respuesta: Se adjunta el Programa de Protección de Datos Personales de la Fiscalía General del Estado de Puebla.

Qué mecanismos han implementado y/o realizado para asegurar que los datos personales se entreguen solo a sus titulares y/o representantes.
Respuesta: De conformidad con lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, y los Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla

Cuantos servidores públicos integran su unidad de transparencia.
Respuesta: 5 personas.

Cuántas auditorías en materia de datos personales le han solicitado al órgano garante desde el 2010 a la fecha.
Respuesta: Cero.

Se me informe si han remitido el informe semestral referente al número de requerimientos de localización geográfica en tiempo real y de registro de datos realizados, así como el número de

registros de datos de comunicaciones cancelados y suprimidos de manera segura, una vez cumplido el fin para el cual fueron solicitados, de los años 2010 a la fecha.
Referente al informe antes solicitado se me entregue el link donde pueda consultar la información estadística de dicho informe.
Respuesta: Por lo que respecta a los dos cuestionamientos que anteceden, le informamos que con fecha **7 de octubre de 2024**, se previno parcialmente esta solicitud de información, a fin de que precisara con toda exactitud**, a qué autoridad, entidad o lugar refiere al indicar:** *"Se me informe si* ***han remitido el informe semestral*** *referente al número de requerimientos de localización geográfica"*; y dado que no se recibió respuesta a dicha prevención, se hizo efectivo el apercibimiento y se tuvieron como no presentados dichos cuestionamientos.

Cuántas denuncias en materia de datos personales han recibido desde los años 2010 a la fecha.
Respuesta: Se cuenta con Cero denuncias.

Se me explique cuáles son las medidas que aplican para uno de los principios incorporados en la LGPDPPSO, para garantizar el tratamiento de los datos personales.
Respuesta: Las medidas aplicadas se encuentran contenidas en el "Documento de Seguridad para la Protección de Datos Personales 2023" y "Documento de Seguridad para la Protección de Datos Personales2024", mismos que se adjuntan.

Qué sujetos obligados han presentado su evaluación de impacto en la protección de datos personales en los años 2020 a la fecha.
Respuesta: Se cuenta con Cero registros de la información solicitada.

Cuantas recomendaciones no vinculantes han emitido sobre el contenido de la evaluación de impacto de los años 2020 a la fecha.
Respuesta: se cuenta con Cero registros de la información solicitada.

Cuántas denuncias en materia de obligaciones de transparencia han recibido desde el año 2020 a la fecha y el sentido de la resolución.
Respuesta: En el periodo solicitado, se cuenta con 2 (dos) denuncias recibidas durante el año 2020, mismas que fueron declaradas infundadas.

Qué programa y/o acciones han implementado en materia de gobierno abierto.
Respuesta: La Fiscalía General del Estado ha implementado diversas acciones mismas que se ven reflejadas en el Portal Web: https://fiscalia.puebla.gob.mx/, en el cual se posee un apartado de "Transparencia", donde se encuentra publicada diversa información de interés público.

Reciba un cordial saludo.

www.fiscalia.puebla.gob.mx /fiscaliapuebla @FiscaliaPuebla
Blvd. Héroes del 5 de Mayo y 31 Oriente, col. Ladrillera de Benítez
C.P. 72530, Puebla, Pue. (222) 211 79 00 Ext. 4019 y 4050

FISCALÍA GENERAL DEL ESTADO DE PUEBLA

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

2023

www.fiscalia.puebla.gob.mx /fiscaliapuebla @FiscaliaPuebla
Blvd. Héroes del 5 de Mayo y 31 Oriente, col. Ladrillera de Benítez
C.P. 72530, Puebla, Pue. (222) 211 79 00 Ext. 4019 y 4050

ÍNDICE

INTRODUCCIÓN.....3

I. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.....4

II. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.....7

III. ANÁLISIS DE RIESGOS.....8

IV. ANÁLISIS DE BRECHA.....9

V. PLAN DE TRABAJO.....10

VI. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.....13

VII. PROGRAMA DE CAPACITACIÓN.....15

INTRODUCCIÓN

Tanto la Ley General de Transparencia y Acceso a la Información Pública, como la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, tienen por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier sujeto obligado, así como garantizar el acceso, rectificación, cancelación y oposición de datos personales por parte de sus titulares, garantizando su protección.

Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados define los datos personales como cualquier información concerniente a una persona física identificada o identificable, para lo que se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. Por otra parte, hace la distinción entre los datos personales sensibles, los cuales define como aquellos que se refieran a la esfera más íntima, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, para enunciar algunos se consideran sensibles los datos que revelan aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas o morales, así como las opiniones políticas o preferencia sexual, etc.

De conformidad con lo dispuesto en el artículo 1 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, es de observancia obligatoria en el Estado de Puebla y tiene por objeto garantizar el derecho que tiene toda persona a la protección de sus Datos Personales.

Para la consecución de su objeto, esta Fiscalía General cuenta con diversas atribuciones, en cuyo ejercicio tiene acceso al tratamiento de diversos datos personales, los cuales se distribuyen en sus respectivos sistemas de tratamientos.

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, establece dentro de sus deberes una serie de medidas de seguridad que los responsables deberán observar en la protección de datos personales, en este sentido, el artículo 51 de la citada Ley, prevén la obligación de elaborar un “documento de seguridad”.

Por lo anterior, la Fiscalía General del Estado de Puebla, con la finalidad de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, emite el presente documento, en observancia de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, con la intención de brindar homogeneidad en la organización y procesos para la protección de los datos personales.

Asimismo, el presente documento tiene como propósito controlar internamente el universo de datos personales en posesión del Instituto, el tipo de datos personales que contienen los archivos, los responsables, las obligaciones, el análisis de riesgos y los mecanismos de monitoreo y revisión de las medidas de seguridad, entre otros.

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

En cumplimiento a lo establecido en los artículos 33, fracción III y 35, fracción I de la Ley General de Datos Personales en Posesión de Sujetos Obligados y 51 de Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, la Fiscalía General del Estado, con la finalidad de establecer y mantener las medidas de seguridad para la protección de los datos personales, emitió el presente inventario de datos personales y de los sistemas de tratamiento, con la información básica del tratamiento de datos personales señalado por las Unidades Administrativas de este Órgano Autónomo.

1. OFICIALÍA MAYOR

1.1 Sistema de Registro de Acceso a las Instalaciones	
Finalidad del tratamiento	Registrar y mantener actualizada la información de las personas que ingresan a las instalaciones de la Fiscalía General.
Datos personales recabados	Nombre, foto, huella digital. (datos personales no sensibles).
Uso de los datos	Mantener un registro de las personas que ingresan a las instalaciones de la Fiscalía General.
Formato de almacenamiento	Electrónico (Base de datos en formato Excel).
Descripción general de ubicación física y/o electrónica	Carpeta compartida de la Oficialía Mayor, en los servidores de la Fiscalía General, únicamente personal facultado por la Oficialía Mayor cuenta con acceso a
Fundamento legal	De conformidad con Lineamientos L/014/2021 de Seguridad Institucional en las Instalaciones de la Fiscalia General del Estado de Puebla Artículos 5, fracciones VIII y XXXV, 14 y 16 de la
Cargo del servidor responsable	Oficial Mayor.

2. UNIDAD DE TRANSPARENCIA

2.1 Sistema de Registro de Solicitudes de Acceso a la Información y Solicitudes ARCO	
Finalidad del tratamiento	Registrar y mantener actualizada la información de las solicitudes que ingresan a través de la Plataforma Nacional de Transparencia y demás habilitados para ello.
Datos personales recabados	Nombre, correo electrónico, sexo. (datos personales no sensibles).
Uso de los datos	Mantener un registro de las solicitudes que son recibidas por la Fiscalía General.
Formato de almacenamiento	Electrónico (Base de datos en formato Excel).
Descripción general de ubicación física y/o electrónica	Carpeta compartida de la Unidad de Transparencia, en los servidores de la Fiscalía General, únicamente personal facultado por la Unidad de Transparencia
Fundamento legal	De conformidad con el articulo 187 fracción IV del Reglamento de la Ley Orgánica de la Fiscalía General del Estado. Artículos 5, fracciones VIII y XXXV, 14 y 16 de la
Cargo del servidor responsable	Titular de la Unidad de Transparencia.

3. COORDINACIÓN GENERAL DE ESTADÍSTICA Y SISTEMAS DE INFORMACIÓN

3.1 Sistema de Control y Evaluación de la Gestión Institucional	
Finalidad del tratamiento	Es una herramienta de inteligencia en procuración de justicia, útil para la toma de decisiones y para evaluar permanentemente la actividad sustantiva de la Institución.
Datos personales recabados	Nombre, sexo, fecha de nacimiento, dirección, teléfono, características fiscas. (datos personales sensibles).

Uso de los datos	El sistema permite llevar en tiempo real el control de la actividad sustantiva de la Institución, mediante el registro de la información relativa a las Carpetas de Investigación y su curso por cada una de las etapas del procedimiento penal.
Formato de almacenamiento	Electrónico (Base de datos).
Descripción general de ubicación física y/o electrónica de los datos personales	Sistema de gestión de la Coordinación General de Estadística y Sistemas de Información, en los servidores de la Fiscalía General, únicamente personal facultado por la Coordinación General de Estadística y Sistemas de Información cuenta con acceso a dicha sistema.
Fundamento legal	De conformidad con el artículo 144 del Reglamento de la Ley Orgánica de la Fiscalía General del Estado. Artículos 5, fracciones VIII y XXXV, 14 y 16 de la LPDPPSOEP.
Cargo del servidor responsable	Coordinadora General de Estadística y Sistemas de Información

II. Funciones y obligaciones de las personas que traten datos personales

De conformidad con el artículo 5, fracción XXXV de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, los servidores públicos de la Fiscalía General que traten datos personales en el ejercicio de sus funciones y de las atribuciones de la Unidad Administrativa a la que se encuentran adscritos observarán, al menos, las medidas de seguridad técnicas siguientes:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

Adicionalmente, los servidores públicos de la Fiscalía General, al tratar los datos personales, observarán las siguientes funciones y obligaciones:

Funciones:

- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- Llevar un registro de los servidores públicos que accedan a los datos personales y llevar a cabo las acciones necesarias para que sea necesaria la autenticación de los usuarios.
- Mantener actualizada la relación de usuarios que traten datos personales.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar dicho incidente a la Unidad de Transparencia de la Fiscalía General y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad de carácter administrativo, físico y técnico necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizando la confidencialidad, integridad y disponibilidad de los mismos.

Atender los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.

III. Análisis de Riesgos

Los datos personales a los que los servidores públicos de la Fiscalía General tienen acceso en el ejercicio de sus atribuciones, se resguardan de manera física y electrónica, según las necesidades de la actividad para la cual se lleva a cabo su tratamiento.

Tanto para la protección de datos personales, como para los datos personales sensibles, determinados junto con su ciclo de vida por las Unidades Administrativas en el "Inventario de Datos Personales y de los Sistemas de Tratamiento" de la Fiscalía General observa el máximo nivel de protección; es decir, sin discriminarlos por su valor o ciclo de vida, pues su vulneración podría tener como consecuencia negativa para los titulares de los datos personales la divulgación o incluso un daño en su esfera más íntima, daño moral o patrimonial, entre otros, siendo que el valor de los datos personales en la actualidad cobra cada día mayor relevancia por las implicaciones e información vinculados a ellos.

En este sentido, tanto los sistemas electrónicos como los medios a través de los cuales se resguardan de manera física los datos personales presentan diferentes particularidades en razón de las características de cada uno de ellos.

Por lo que hace a los datos personales que se resguardan de manera física, los riesgos existentes son la pérdida o uso indebido de la información, deterioro negligente, así como su destrucción; por ello, la Fiscalía General cuenta con un área soporte encargada de ejecutar acciones para garantizar la seguridad de la información, manteniendo en un mínimo su exposición, pues únicamente pueden acceder a ellos los servidores públicos facultados y con acreditación para su uso.

Por su parte, los datos personales contenidos en un sistema electrónico presentan riesgos por su propia naturaleza como lo son el uso indebido de la información, la falla en los equipos electrónicos o en los sistemas; por ello, la Fiscalía General cuenta con un área soporte encargada de ejecutar acciones para garantizar la seguridad de la información, manteniendo en un mínimo su exposición, pues únicamente pueden acceder a ellos los servidores públicos facultados y previa acreditación de su personalidad a través de medios electrónicos para su uso.

IV. Análisis de brecha

Las medidas de seguridad existentes y efectivas para la protección de datos personales con las que actualmente cuenta la Fiscalía General, son las siguientes:

1. Medidas de seguridad: La información que contiene datos personales se resguarda en una ubicación que cuenta con diversas medidas de seguridad como cámaras de seguridad, archiveros específicos para su resguardo y uso de cerraduras para su acceso.
2. Medidas de control: Medidas de carácter administrativo encaminadas a contar con un registro físico de los servidores públicos que tienen acceso a datos personales, así como de los datos personales contenidos en los documentos.
3. Medidas legales: Cuando se lleva a cabo la transferencia de datos personales entre sujetos obligados o entre servidores públicos de la Fiscalía General, se realiza el apercibimiento en cuanto al trato que se le deberá dar a los mismos, en los términos de la legislación vigente en la materia.
4. Medidas cibernéticas: La Coordinación General de Estadística y Sistemas de Información, cuenta con atribuciones para establecer normas y lineamientos e implementar esquemas de seguridad para la infraestructura de tecnología de la información, comunicaciones y sistemas que permitan garantizar conexiones seguras, tanto al exterior como al interior de la Fiscalía General.

A efecto de fijar la brecha entre las medidas de seguridad con las que cuenta la Fiscalía General y las faltantes y/o nuevas por implementar, se han identificado las siguientes:

1. Implementar en los siguientes planes de capacitación de personal, nuevos cursos o programas enfocados a la protección de datos personales.
2. Designar a un responsable para la rendición de cuentas de la gestión de los datos personales, de modo que tanto el cumplimiento de la legislación en protección de datos personales, como la política de gestión y seguridad de datos personales, puedan ser demostrados.
3. El responsable designado para la protección de datos personales, deberá estar a cargo del cumplimiento de la política de protección de datos personales de manera cotidiana.
4. Implementar mecanismos o programas tecnológicos novedosos para garantizar las amenazas que se presenten en materia de ciberseguridad en el futuro.
5. Se deben designar deberes y obligaciones respecto a los servidores públicos que intervengan en el uso y protección de datos personales.

V. Plan de Trabajo

Atendiendo a lo dispuesto en el análisis de riesgo y el análisis de brecha desarrollado en el presente documento y con la intención de definir las acciones a implementar para garantizar la protección de datos personales, se formuló el plan de trabajo siguiente:

Acciones	Temporalidad	Responsable	Descripción
Medidas cotidianas de protección de datos personales			
Gestión de datos personales	Permanente	Usuario de los datos personales	Se respetarán las medidas implementadas para el mantenimiento de los diferentes controles establecidos para salvaguardar los datos personales relacionados durante su tratamiento.
Prevención del mal uso de activos informáticos	Permanente	Coordinación General de Estadística y Sistemas de Información	Se deben tener mecanismos contra el uso de activos para propósitos no autorizados, como son los sistemas electrónicos, la utilización de bloqueos en caso de que usuarios no autorizados traten de acceder a módulos que no tienen permitido.
Cumplimiento legal			
Identificación de legislación	Al momento de iniciar el	Usuario de los datos	Se identificarán los deberes y responsabilidades para

aplicable	tratamiento de datos personales	personales con auxilio de ser necesario de la Coordinación General de Asuntos Jurídicos	cumplir con los requerimientos legales relacionados con la protección de datos personales.
Actualización de registro de usuarios	Cada que se lleven a cabo modificaciones	Encargado del registro de cada Unidad Administrativa	Se deben mantener actualizados los registros de los usuarios de datos personales.

Acciones	Temporalidad	Responsable	Descripción
Comunicación permanente al momento de llevar a cabo transferencia de datos personales	Al momento de que se lleve a cabo la transferencia de datos personales	Los servidores públicos que realicen la transferencia	Cuando se lleva a cabo la transferencia de datos personales entre sujetos obligados o entre servidores públicos de la Fiscalía General, se realizará el apercibimiento en cuanto al trato que se le deberá dar a los mismos, en los términos de la legislación vigente en la materia.
Recomendaciones en materia de seguridad de la información	Al momento de identificarlas	Personal de la Unidad de Transparencia	Cuando sea adecuado, obtener el consejo y recomendaciones de un especialista en protección de datos y seguridad de la información.
Acompañamiento	Al momento de que acontezca una contingencia	Personal adscrito a la Unidad de Transparencia y a la Coordinación General de Asuntos Jurídicos	Se llevará a cabo el acompañamiento y asesoría del personal adscrito a la Unidad de Transparencia y a la Coordinación General de Asuntos Jurídicos al momento de llevar a cabo las acciones apropiadas en caso de un incidente o vulneración de seguridad.

Estructura organizacional			
Designación de deberes en seguridad y protección de datos personales	Al momento de identificarlas	Titulares de las Unidades Administrativas	Se deben designar deberes y obligaciones respecto a los servidores públicos que intervengan en el uso y protección de datos personales.
Contratos con proveedores	Permanente	Área contratante	En la elaboración de los contratos con proveedores, revisar las cláusulas referentes a los requerimientos de seguridad y de tratamiento de datos personales para verificar su correspondencia con los requerimientos de la Fiscalía General.
Seguridad del personal			
Capacitación	Anualmente	Unidad de Transparencia	Los servidores públicos de la Unidad de Transparencia privilegiarán la asesoría en materia de datos personales para los servidores públicos de la Fiscalía General, incluyéndolos en su plan anual de capacitación.
Resguardo de la documentación	Permanente	Usuario de los datos personales	Cualquier documento o activo de información crítico debe estar resguardado, fuera de la vista, cuando éste no sea atendido.

VI. Mecanismos de monitoreo y revisión de las medidas de seguridad

En el presente documento de seguridad para la protección de datos personales, se detallan las acciones que establecen el mantenimiento de las medidas de seguridad en las cuales de manera general se destaca que el objeto de las mismas es la protección de los datos personales.

Para ello, con la finalidad de mantener un monitoreo y revisión de las medidas de seguridad, se llevarán a cabo de manera permanente las acciones siguientes:

1. La Unidad de Transparencia llevará un monitoreo del cumplimiento por parte de los servidores públicos que intervengan en las actividades detalladas en el Plan de Trabajo del presente documento.
2. Se mantendrá actualizado el inventario de datos personales y de los sistemas de tratamiento de los mismos.
3. La Coordinación General de Estadística y Sistemas de Información, mantendrá monitoreados los esquemas de seguridad implementados para la infraestructura de tecnología de la información, comunicaciones y sistemas que permitan garantizar conexiones seguras, tanto al exterior como al interior del Instituto.
4. Para garantizar el cumplimiento de las políticas en materia de protección de datos personales establecidas en el presente documento de seguridad, el mismo se publicará en la Intranet Institucional de la Fiscalía General y se enviará por medios electrónicos a los servidores públicos de la Institución.
5. Se llevarán a cabo diversas medidas de seguridad físicas para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento mediante las siguientes actividades:
    - Prevenir el acceso no autorizado al perímetro del lugar en que se resguarden los datos personales en sus instalaciones físicas.
    - Prevenir el daño o interferencia a las instalaciones físicas, recursos e Información.
    - Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir de las instalaciones de la organización.
    - Proveer a los equipos que contienen o almacenan datos personales de un
    - mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.
6. En relación con el monitoreo de la seguridad se observará lo dispuesto en el artículo 48 fracción VII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, el cual establece que deberá 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.

   En este sentido, las acciones a monitorear son las siguientes:

- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica entre otras.
- Las nuevas amenazas que podrían estar activadas dentro y fuera de la organización y que no han sido valoradas.
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas pasadas que vuelvan a surgir.
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

VII. Programa de capacitación

La Fiscalía General del Estado, ha promovido la capacitación de los servidores públicos en materia de protección de datos personales, mediante los Cursos de Formación Inicial, impartido por la Unidad de Transparencia, adquiriendo los conocimientos de los aspectos fundamentales de la Ley, con la finalidad de garantizar el derecho a la protección de los mismos.

En este sentido, se busca continuar con la promoción de la capacitación en la materia, a través de los cursos citados e incluir con el apoyo del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Puebla (ITAIPUE), nuevos cursos que permitan ampliar los conocimientos adquiridos por los servidores públicos de la Fiscalía General, por lo que se continuará en constante comunicación con el citado Instituto para tales efectos.

- Cronograma de capacitación

NÚMERO	UNIDAD ADMINISTRATIVAS
1	Fiscalía Especializada en Derechos Humanos
2	Fiscalía de Investigación Metropolitana
3	Fiscalía de Investigación Regional
4	Fiscalía Especializada en Investigación de los Delitos de Desaparición Forzada de Personas y Desaparición Cometida por Particulares
5	Fiscalía Especializada en Investigación de Secuestro y Extorsión
6	Fiscalía Especializada de Combate a la Corrupción
7	Fiscalía Especializada en Investigación de Delitos Electorales
8	Fiscalía Especializada en Investigación de Delitos de Alta Incidencia
9	Fiscalía Especializada en Investigación de Delitos de Violencia de Género contra las Mujeres
10	Fiscalía Especializada de Asuntos Internos
11	Fiscalía Especializada en Investigación de los Delitos de Operaciones con Recursos de Procedencia Ilícita, Fiscales y Relacionados
12	Oficialía Mayor
13	Agencia Estatal de Investigación
14	Instituto de Ciencias Forenses
15	Órgano Interno de Control
16	Visitaduría General
17	Instituto de Formación Profesional

18	Coordinación General Especializada en Investigación de Robo de Vehículos
19	Coordinación General Especializada en Investigación de Homicidios Dolosos
20	Coordinación General de Mecanismos Alternativos de Solución de Controversias en Materia Penal
21	Coordinación General de Análisis de Información
22	Coordinación General de Colaboración Interinstitucional
23	Coordinación General de Estadística y Sistemas de Información
24	Coordinación General de Gestión Documental Institucional
25	Coordinación General de Asuntos Jurídicos
26	Coordinación General de Servicios a la Comunidad
27	Coordinación General de Investigación
28	Coordinación General de Litigación
29	Coordinación General de Desarrollo Institucional
30	Dirección General de Seguridad Institucional
31	Dirección General de Planeación Institucional
32	Dirección General de Comunicación Estratégica y Vinculación Social
33	Unidad Especializada en Materia de Extinción de Dominio

Junio						
Do	**Lu**	**Ma**	**Mi**	**Ju**	**Vi**	**Sa**
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Julio						
Do	**Lu**	**Ma**	**Mi**	**Ju**	**Vi**	**Sa**
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15

16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

www.fiscalia.puebla.gob.mx /fiscaliapuebla @FiscaliaPuebla

Blvd. Héroes del 5 de Mayo y 31 Oriente, col. Ladrillera de Benítez
C.P. 72530, Puebla, Pue. (222) 211 79 00 Ext. 4019 y 4050

FISCALÍA GENERAL DEL ESTADO DE PUEBLA

PROCEDIMIENTO PARA LA CONSERVACIÓN, MODIFICACIÓN Y SUPRESIÓN DE DATOS PERSONALES

www.fiscalia.puebla.gob.mx /fiscaliapuebla @FiscaliaPuebla
Blvd. Héroes del 5 de Mayo y 31 Oriente, col. Ladrillera de Benítez
C.P. 72530, Puebla, Pue. (222) 211 79 00 Ext. 4019 y 4050

ÍNDICE

I. PRESENTACIÓN..... 3

II. OBJETIVOS GENERALES..... 3

III. MARCO LEGAL..... 3

IV. GLOSARIO..... 3

V. PROCEDIMIENTO..... 6

A) DE LA CONSERVACIÓN DE DATOS PERSONALES..... 6

B) DE LA MODIFICACIÓN DE DATOS PERSONALES 7

C) DE LA SUPRESIÓN DE DATOS PERSONALES..... 8

INTRODUCCIÓN

Derivado del cúmulo de datos personales que recaban las áreas de la Fiscalía General del Estado de Puebla como sujeto obligado, en cumplimiento a las funciones y atribuciones que la normatividad aplicable les confiere, la Unidad de Transparencia se ve en la necesidad de implementar las acciones conducentes para garantizar una mayor eficacia en el tratamiento de los datos que llevan a cabo las áreas, acorde a sus finalidades, funciones y atribuciones descritas en la normatividad aplicable. Por esta razón, y de conformidad con lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, dicha Unidad propone Procedimiento para la Conservación, Modificación, Supresión y Actualización de Datos Personales de la Fiscalía General del Estado de Puebla.

Este documento permitirá que las áreas conozcan y ejecuten el procedimiento para la conservación, modificación, supresión y actualización de datos personales.

Para el desarrollo del procedimiento señalado, la Unidad de Transparencia orientará y acompañará en todo momento a las áreas que administren datos personales e instrumentará conforme al programa anual de actividades o a las necesidades institucionales, las capacitaciones que se requieran a las áreas administradoras, para atender de manera eficiente la actualización de los sistemas o bases de datos personales que recaban.

II. OBJETIVO GENERAL

· Establecer el procedimiento para la conservación, modificación, supresión y actualización de datos personales que administran las áreas, conforme a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla.

Objetivos específicos

· Precisar los pasos a seguir para llenar de manera correcta la cédula de creación, modificación, actualización y supresión de los sistemas y/o bases de datos personales.

· Colaborar con las áreas administrativas de la Fiscalía General de Estado para determinar, a través del Comité de Transparencia, la conservación, modificación o supresión de datos personales, conforme a su respectivo ámbito de competencia, el análisis de los datos personales que recaban.

III. MARCO LEGAL

En la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla se establece que:

El Responsable deberá establecer y documentar los procedimientos para la conservación, y en su caso Bloqueo y supresión de los Datos Personales en su posesión, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en

el artículo anterior de la presente Ley.

En los procedimientos a que se refiere el párrafo anterior, el Responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los Datos Personales, así como para realizar una revisión periódica sobre la necesidad de conservar los Datos Personales.

Todo Tratamiento de Datos Personales que efectúe el Responsable deberá estar justificado por finalidades concretas, explícitas, lícitas y legítimas, relacionadas con las atribuciones expresas que la normativa aplicable le confiera. Para efectos de la presente Ley, se entenderá que las finalidades son:

> I. Concretas: cuando el Tratamiento de los Datos Personales atiende a la consecución de fines específicos o determinados, sin que sea posible la existencia de finalidades genéricas que puedan generar confusión en el Titular;
> II. Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el Aviso de Privacidad, y
> III. Lícitas y legítimas: cuando las finalidades que justifican el Tratamiento de los Datos Personales son acordes con las atribuciones expresas del Responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable.

IV. GLOSARIO

Áreas: Instancias de los Responsables previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan con facultades y/o atribuciones para dar Tratamiento a los Datos Personales.

Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el Responsable, que es puesto a disposición del Titular con el objeto de informarle las características principales del Tratamiento al que serán sometidos sus Datos Personales;

Base de Datos: Conjunto ordenado de Datos Personales referentes a una persona física identificada o identificable, condicionado a criterios determinados que permitan su Tratamiento, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Comité: Comité de Transparencia de la Fiscalía General del Estado de Puebla.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

Derechos ARCO: Los derechos de acceso, rectificación y cancelación de Datos Personales,

así como la oposición al Tratamiento de los mismos.

Días: a los días hábiles.

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

Documentos: A los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, convenios, contratos, instructivos, notas, memorándums, estadísticas, o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en formato escrito, sonoro, visual, electrónico, informático, holográfico o de tecnología de información existente.

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

Encargado o encargada: restador de servicios, que con el carácter de persona física o jurídica pública o privada, ajena a la organización del Responsable, trata Datos Personales a nombre y por cuenta de éste.

Fiscalía: Fiscalía General del Estado de Puebla.

Instituto de Transparencia: El Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Puebla

Ley: A la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla.

Ley de Transparencia: A la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla.

Ley Orgánica: Ley Orgánica de la Fiscalía General del Estado.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan garantizar la confidencialidad, disponibilidad e integridad de los Datos Personales.

Reglamento de la Ley Orgánica: Reglamento de la Ley Orgánica de la Fiscalía General del Estado de Puebla.

Responsable: Fiscalía General de Estado de Puebla.

Supresión: La baja archivística de los Datos Personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los Datos Personales bajo las medidas de seguridad previamente establecidas por el Responsable.

Titular de los datos: A la persona física a quien hacen referencia o pertenecen los Datos Personales objeto del Tratamiento establecido en la presente Ley.

Transferencia: Toda comunicación de Datos Personales dentro o fuera del territorio mexicano, realizada a persona distinta del Titular, del Responsable o del Encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los Datos Personales, relacionadas, de manera enunciativa mas no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, Transferencia y en general cualquier uso o disposición de Datos Personales.

Unidad de Transparencia: Unidad de Transparencia de la Fiscalía General del Estado de Puebla

V. PROCEDIMIENTO

A) De la conservación de datos personales

Cuando las áreas recaben datos personales con el objeto de dar cumplimiento a las atribuciones legales:

1. Deberán solicitar a la Unidad de Transparencia, mediante oficio y a través de sus titulares, la creación del sistema y/o base de datos personales, así como la clasificación de los datos que sean objeto de tratamiento, precisando los que tienen el carácter de no confidenciales, por lo menos con cinco días hábiles de anticipación a la implementación del sistema y/o base de datos personales.

Cuando se solicite la creación de una base de datos personales, se deberá especificar el sistema de datos personales al que se incorporará.

A la solicitud señalada, se deberán adjuntar las propuestas de avisos de privacidad integral y simplificado en archivo Word, conforme a los formatos y guía aprobados por el Comité para que sean publicados en el portal de Transparencia y Acceso a la Información, acompañados con el formato, formulario, documento o medio por el cual se recabarán los datos personales.

Cuando las propuestas de avisos de privacidad se encuentren acordes a los formatos aprobados por el Comité y la Ley de Datos Personales del Estado, la Unidad de Transparencia

informará al área, mediante oficio, lo conducente para que proceda a su utilización. En caso de que existieran observaciones, estas serán remitidas al área para que, una vez impactadas, se remitan los avisos de privacidad corregidos a la Unidad de Transparencia para su validación y publicación.

2. Recibida la solicitud, la Unidad de Transparencia procederá a realizar su revisión y elaborará el proyecto de acuerdo por el que se crea el sistema y/o base de datos personales y se clasifican como confidenciales los datos personales contenidos en el mismo. Cuando se vaya a crear una base de datos, se deberá puntualizar a cuál sistema de datos personales se incorporará.

En caso de que la Unidad de Transparencia detecte inconsistencias, realizará los ajustes necesarios en el proyecto de acuerdo respectivo.

3. La Unidad de Transparencia someterá a consideración del Comité el proyecto de acuerdo, para que, en su caso, apruebe la creación del sistema y/o bases de datos personales y la clasificación de los datos personales que serán objeto de tratamiento como confidenciales, conforme la Ley de Datos Personales del Estado.

Si se realizaron ajustes al sistema y/o base de datos mediante el acuerdo emitido por el Comité, las áreas deberán remitir a la Unidad de Transparencia nuevamente la documentación con las modificaciones precisadas, en un plazo no mayor a los cinco días hábiles siguientes a la notificación del acuerdo.

B) De la modificación de datos personales

1. La modificación a los sistemas y/o bases de datos personales se realizará cuando las áreas realicen ajustes al tratamiento de datos personales con motivo de acciones correctivas y preventivas respecto de:

a) La denominación del sistema y/o base de datos personales;
b) El tipo de datos personales que se recaban;
c) El área a la cual corresponderá el sistema y/o base de datos personales;
d) A las o los encargados;
e) La normatividad aplicable que da fundamento al tratamiento de los datos personales;
f) Las finalidades del tratamiento;
g) El uso, origen, forma de recolección, actualización y tiempo de conservación de los datos;
h) El modo de interrelacionar la información registrada, o en su caso, la trazabilidad de los datos;
i) El nivel de seguridad (básico, medio, alto);
j) Las condiciones de las transferencias;

2. La persona titular del área deberán solicitar, mediante oficio, a la Unidad de Transparencia, la modificación del sistema y/o base de datos personales, señalando los

apartados a modificar, de acuerdo con los supuestos previstos en el numeral anterior.

En caso de que haya ajustes en el tipo de datos objeto de tratamiento, las áreas señalarán los datos que serán adicionados especificando los datos confidenciales y los que no tienen el carácter de confidencial.

A la solicitud señalada, se deberán adjuntar las propuestas de avisos de privacidad integral y simplificado en archivo Word, conforme a los formatos y guía aprobados por el Comité, para que sean publicados en el portal de Transparencia.

Cuando las propuestas de avisos de privacidad se encuentren acordes, los formatos aprobados por el Comité y la Ley de Datos Personales del Estado, la Unidad de Transparencia informará al área, mediante oficio, lo conducente para que proceda a su utilización. En caso de que existieran observaciones estas serán remitidas al área para que, una vez impactadas se remitan los avisos de privacidad corregidos a la Unidad de Transparencia para su validación y publicación.

3. Una vez recibida la solicitud, la Unidad de Transparencia procederá a realizar su revisión y elaborará el proyecto de acuerdo por el que se modifica la base de datos personales. En caso de que la Unidad de Transparencia detecte inconsistencias, realizará los ajustes necesarios en el proyecto de acuerdo respectivo.

Asimismo, en el caso de que el área incluya en su solicitud de modificación nuevos datos personales que serán objeto de tratamiento de los cuales no se haya analizado su clasificación en el Acuerdo de creación del sistema y/o base de datos personales, dichos datos serán analizados por la Unidad de Transparencia en el Acuerdo por el cual se realice la modificación.

4. La Unidad de Transparencia someterá a consideración del Comité el proyecto de acuerdo, para que, en su caso, apruebe la modificación del sistema y/o bases de datos personales.

Si se realizaron ajustes a la base de datos mediante el acuerdo emitido por el Comité, las áreas deberán remitir a la Unidad de Transparencia nuevamente la documentación con los ajustes precisados, en un plazo no mayor a cinco días hábiles siguientes a la notificación del acuerdo.

C) De la supresión de datos personales

1. Cuando los datos personales dejen de ser necesarios para las finalidades que fueron recabados y haya concluido su plazo de conservación establecido por los instrumentos de control archivísticos y la normatividad específica aplicable, las áreas podrán solicitar a la Unidad de Transparencia la supresión de los datos personales.

2. Quienes sean titulares de las áreas determinarán la técnica que utilizarán para el borrado seguro de los datos personales, dependiendo el tipo de soporte (físico o electrónico) en el que se encuentran contenidos,

3. Las áreas serán responsables del destino de los datos personales y de las previsiones que se adopten para su destrucción. De la citada destrucción de los datos personales podrán ser excluidos aquellos que, con finalidades estadísticas o históricas, sean previamente sometidos al procedimiento de disociación.

La supresión de datos personales no procederá en caso de que exista una previsión expresa en una Ley o demás normatividad aplicable, o bien, cuando su plazo de conservación contenido en los instrumentos de control archivístico y vigencia documental no haya fenecido.

4. La Unidad de Transparencia elaborará el proyecto de acuerdo de supresión de los datos personales, lo cual será sometido a consideración del Comité. En caso de que la Unidad de Transparencia detecte inconsistencias, realizará los ajustes necesarios en el proyecto de acuerdo respectivo.

5. La Unidad de Transparencia someterá a consideración del Comité el proyecto de acuerdo, para que, en su caso, apruebe la supresión de datos personales, conforme al primer párrafo del artículo 29 de la Ley.

6. Las áreas serán las responsables de instrumentar operativamente la supresión y cancelación de datos personales, para lo cual notificarán a la Unidad de Transparencia, mediante oficio, el lugar, día y hora en que tendrá verificativo la destrucción.

7. La Unidad de Transparencia a través del oficial de protección de datos levantará acta circunstanciada de la destrucción, en la que el personal de cada una de las áreas señaladas y el propio oficial de protección de datos personales firmarán de asistencia.

FISCALÍA GENERAL DEL ESTADO DE PUEBLA

PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES.

ÍNDICE

INTRODUCCIÓN. 3

MARCO JURÍDICO. 3

GLOSARIO. 4

OBJETIVO. 6

RESPONSABILIDADES DENTRO DEL PROGRAMA. 6

ALCANCE DEL PROGRAMA. 7

CUMPLIMIENTO DE OBLIGACIONES. 7

FUNCIONES DEL COMITÉ DE TRANSPARENCIA. 10

FUNCIONES DE LA UNIDAD DE TRANSPARENCIA. 11

CAPACITACIÓN. 12

REVISIONES Y AUDITORIAS. 12

LA DEFINICIÓN DE ACCIONES PARA LA MEJORA CONTINUA. 12

SANCIONES..... 12

INTRODUCCIÓN

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada hasta el 26 de enero de 2017, constituye la materialización de la reforma constitucional de 2014. Por medio de ésta se desarrollan los principios, bases y procedimientos establecidos por nuestra carta magna por lo que se refiere al derecho a la protección de datos personales en posesión de los sujetos obligados. Se trata del marco jurídico general aplicable de manera directa a la Federación y a partir del cual los estados adoptan su propio régimen legal y se emiten las diversas medidas regulatorias en los distintos órdenes de gobierno.

En tales consideraciones, la Fiscalía General del Estado de Puebla como sujeto obligado y responsable en el tratamiento de datos personales que conforme a sus atribuciones lleve a cabo, garantizará la privacidad de los individuos.

Así, entre las acciones que debe realizar la Fiscalía General como responsable del tratamiento de datos personales, y con la finalidad de cumplir con el principio de responsabilidad, se encuentra la elaboración de políticas y programas de protección de datos personales, a fin de implementar mejores prácticas al interior de la organización, por lo que, para la elaboración del presente Programa de Protección de Datos Personales, se identificaron las obligaciones que se deben cumplir y los principios que se deben observar en el tratamiento de datos personales, conforme a la etapa del ciclo de vida de los datos personales; lo anterior, conforme a lo que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, y demás normatividad que regula la materia, y a partir de ello, se definieron las acciones a seguir para su cumplimiento.

Finalmente, el presente Programa está basado en un sistema de gestión que permite proveer los elementos y actividades de dirección, operación y control de los procesos este órgano autónomo, para proteger de manera sistemática y continua los datos personales que estén en su posesión, entendiendo como un sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, así como, el cumplimiento de los principios, deberes y obligaciones previstos en dicha ley y las demás disposiciones que resulten aplicables en la materia.

MARCO JURÍDICO.

Constitución Política:

1. Constitución Política de los Estados Unidos Mexicanos.

Leyes:

1. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
2. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de

Puebla.
3. Ley Orgánica de la Fiscalía General del Estado.

Reglamento:

1. Reglamento de la Ley Orgánica de la Fiscalía General del Estado.
2. Reglamento Interior de la Fiscalía General del Estado.

GLOSARIO.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva para determinar el grado de cumplimiento de los criterios preestablecidos para la misma.

Aviso de privacidad: Documento físico, electrónico o en cualquier otro formato generado por el Responsable, que es puesto a disposición del Titular con el objeto de informarle las características principales del Tratamiento al que serán sometidos sus Datos Personales.

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

Comité de Transparencia: Instancia a la que hace referencia el artículo 20 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad puede determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

Datos personales sensibles: Aquéllos que se refieren a la esfera más íntima de su Titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. Se consideran sensibles, de manera enunciativa mas no limitativa, los Datos Personales que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, creencias religiosas, filosóficas y morales, opiniones políticas, datos genéticos o datos biométricos.

Derechos ARCO: Los derechos de acceso, rectificación y cancelación de Datos Personales, así como la oposición al Tratamiento de los mismos.

Documento de Seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el Responsable para garantizar la confidencialidad, integridad y disponibilidad de los Datos Personales que

posee.

Encargado: Prestador de servicios, que con el carácter de persona física o jurídica pública o privada, ajena a la organización del Responsable, trata Datos Personales a nombre y por cuenta de éste.

Evaluación de impacto en la protección de datos personales: Documento mediante el cual se valoran y determinan los impactos reales respecto de determinado Tratamiento de Datos Personales, a efecto de identificar, prevenir y mitigar posibles riesgos que puedan comprometer el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en la presente Ley y normativa aplicable en la materia.

Fiscalía: Fiscalía general del Estado de Puebla.

Instituto de Transparencia: Instituto de Transparencia, Acceso a la Información y Protección de Datos Personales del Estado de Puebla.

Incidente: Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas del Fiscalía, que afecte la confidencialidad, la integridad o la disponibilidad de los datos personales.

Ley: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla.

Lineamientos Generales: Lineamientos Generales en Materia de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan garantizar la confidencialidad, disponibilidad e integridad de los Datos Personales.

Programa: Programa de Protección de Datos Personales.

Responsable: Cualquier Unidad Administrativa de la Fiscalía, que decide y determina los fines, medios y demás cuestiones relacionadas con determinado Tratamiento de Datos Personales.

Remisión: Toda comunicación de Datos Personales realizada exclusivamente entre el Responsable y Encargado, dentro o fuera del territorio mexicano.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Titular: Titular: A la persona física a quien hacen referencia o pertenecen los Datos Personales objeto del Tratamiento establecido en la presente Ley.

Transferencias: oda comunicación de Datos Personales dentro o fuera del territorio

mexicano, realizada a persona distinta del Titular, del Responsable o del Encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los Datos Personales, relacionadas, de manera enunciativa mas no limitativa, con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, Transferencia y en general cualquier uso o disposición de Datos Personales.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 15 de la Ley de Transparencia.

Vulnerabilidad: La circunstancias o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño.

Vulneración de seguridad: El incidente de seguridad que afecta a los datos personales en cualquier fase de su tratamiento.

OBJETIVO.

La finalidad del Programa consiste en que la Fiscalía garantice permanentemente que el tratamiento que realiza de los datos personales en su posesión se adecue y cumpla con los principios y obligaciones previstos en la Ley, en los Lineamientos Generales y demás normatividad aplicable en la materia.

A efecto de lograr lo señalado, se han trazado los siguientes objetivos:

- Proveer: Los insumos necesarios para que la Fiscalía cuente con los elementos suficientes para asegurar la efectividad de los procesos internos para el tratamiento y la seguridad de los datos personales en posesión de las unidades administrativas que lo conforman.
- Cumplir: Con las obligaciones establecidas en la Ley, Lineamientos Generales y demás normatividad que regula la materia.
- Promover: La adopción de buenas prácticas en la protección de datos personales.
- Establecer: Los procesos que impliquen el tratamiento de datos personales para tener un control efectivo

RESPONSABILIDADES DENTRO DEL PROGRAMA.

De conformidad con lo dispuesto en los artículos 113 y 114, fracción I de la Ley; el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales, y dentro de sus funciones se encuentra el coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la

organización de la Fiscalía.

Por ello, dicho Órgano Colegiado tendrá, en relación con este programa, las funciones siguientes:

I. Aprobar, coordinar y supervisar el Programa;

II. Proponer cambios y mejoras al Programa a partir de la experiencia de su implementación;

III. Dar a conocer el Programa al interior del sujeto obligado a través de la Unidad de Transparencia;

IV. Coordinar la implementación del Programa en las unidades administrativas de la Fiscalía;

V. Asesorar a las áreas competentes en la implementación de este Programa con el apoyo de la Unidad de Transparencia;

VI. Aprobar el programa anual de capacitación;

VII. Llevar a cabo una revisión de las acciones realizadas para cumplir con lo dispuesto en este Programa; lo anterior, con el apoyo de la Unidad de Transparencia; y

VIII. Las demás que de manera expresa señale el propio Programa.

ALCANCE DEL PROGRAMA.

El presente programa aplicará a todas las unidades administrativas que realicen tratamiento de datos personales en ejercicio de sus atribuciones, quienes además deberán de cumplir con los principios, deberes y obligaciones establecidas en la normatividad que regula la materia. Quedan exceptuados de la aplicación de este programa, los datos personales que correspondan al cumplimiento de las obligaciones de transparencia a las que refieren el artículo 120 de la Ley General de Transparencia y Acceso a la Información Pública y numeral 77 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla.

Este Programa es de observancia obligatoria para todas las personas servidoras públicas que en el ejercicio de sus funciones realicen el tratamiento de datos personales en la Fiscalía.

CUMPLIMIENTO DE OBLIGACIONES.

Se deberán observar las siguientes:

A. Obligaciones transversales. Los deberes de seguridad y confidencialidad deben observarse en cualquier etapa del ciclo de vida de los datos personales. Estas obligaciones

se cumplen a través de los siguientes:

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

2. Vulneraciones. Se considera como vulneración las siguientes:

   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.

Cuando ocurra una vulneración, la Fiscalía debe informar al titular de los datos personales de las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, ello en cuanto se confirme que ocurrió la vulneración y siempre que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

3. Principios. Se deberán observar los siguientes principios durante todas las etapas del ciclo del tratamiento de los datos personales, a saber:

   a) Confidencialidad. Establecer controles o mecanismos para que todas las personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad, obligación que subsistirá aún después de finalizar sus relaciones con el mismo y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.
   b) Responsabilidad. Implementar las siguientes acciones para acreditar el cumplimiento de los principios, deberes y obligaciones, así como para rendir cuentas:

   - Autorizar y destinar recursos para la instrumentación de programas y políticas de protección de datos personales.
   - Elaborar políticas y programas de protección de datos personales.
   - Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.
   - Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.
   - 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.
   - Establecer procedimientos para recibir y responder dudas y quejas

de los titulares.

- Diseñar, desarrollar e implementar las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y
- Garantizar que las políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la Ley, los Lineamientos Generales y las demás que resulten aplicables en la materia.

B. Obligaciones relevantes

1. En la etapa de obtención de los datos personales, se deben observar los siguientes principios:

   a. Licitud. Tratar los datos personales que posea la Fiscalía sujetándose a las atribuciones o facultades de la normatividad aplicable.
   b. Lealtad. Obtener los datos sin dolo, mala fe, engaño o negligencia.
   c. Información. Poner a disposición del titular el aviso de privacidad al momento de la obtención de los datos personales. Difundir el aviso de privacidad por medios electrónicos y físicos. El aviso de privacidad deberá estar redactado conforme a la normatividad en materia de datos personales, para sus dos versiones integral y simplificado.
   d. Consentimiento. Contar con el consentimiento del titular, para el tratamiento de sus datos personales, salvo que se actualice alguna de las excepciones previstas en el artículo 20 (excepciones para la obtención del consentimiento) de la Ley. (Se debe considerar: Consentimiento menores de edad y personas en estado de interdicción o incapacidad declarada conforme a la Ley). Para este principio resulta importante resaltar que no se deben tratar datos personales sensibles salvo que se cuente con el consentimiento expreso del titular o se trate de los casos establecidos en el artículo 20 de la Ley.
   e. Proporcionalidad. Tratar los datos personales sólo cuando resulten adecuados, relevantes y necesarios para la finalidad que justifica su tratamiento. Se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención.

2. En la etapa de uso de los datos personales, se deben observar los siguientes principios:

a. Finalidad. Justificar el tratamiento de los datos personales en finalidades concretas, lícitas, explícitas y legítimas. Se entenderá que las finalidades son:

- Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.
- Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.
- Lícitas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades de la Unidad Administrativa que corresponda.
- Legítimas: cuando las finalidades que motivan el tratamiento de los datos personales se encuentren habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 20 de la Ley.

b. Calidad. Adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales, principalmente cuando se obtuvieron de manera indirecta del titular. Se entenderá que los datos personales son:

-Exactos y correctos: cuando los datos personales en posesión del responsable no presentan errores que pudieran afectar su veracidad.
- Completos: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable.
- Actualizados: cuando los datos personales responden fielmente a la situación actual del titular.

3. En la etapa de eliminación de los datos personales, se deben observar los siguientes principios:

a. Supresión de datos personales. Suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades y una vez que concluya su plazo de conservación establecido.

FUNCIONES DEL COMITÉ DE TRANSPARENCIA.

El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales al interior de la Fiscalía, y al respecto, tendrá las siguientes funciones:

I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho

a la protección de los datos personales en la Fiscalía, de conformidad con las disposiciones previstas en la Ley y en aquellas disposiciones que resulten aplicables en la materia;

II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;

III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;

IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la Ley y en aquellas disposiciones que resulten aplicables en la materia;

V. Supervisar, en coordinación con las unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;

VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto de Transparencia;

VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y

VIII. Dar vista al órgano interno de control en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen las unidades administrativas.

FUNCIONES DE LA UNIDAD DE TRANSPARENCIA.

La Unidad de Transparencia tendrá las siguientes funciones en materia de protección de datos personales:

I. Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;

II. Gestionar las solicitudes para el ejercicio de los derechos ARCO;

III. Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;

IV. Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;

V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO; y

VI. Asesorar a las unidades administrativas en materia de protección de datos personales.

CAPACITACIÓN.

Se establecerá un programa de capacitación y actualización en materia de protección de datos personales, dirigido tanto a personal como a encargados. El programa de capacitación deberá ser a corto, mediano y largo plazo y considerar los roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales y el perfil de puestos.

REVISIONES Y AUDITORIAS.

Se deberá de contar con un programa para llevar a cabo dos tipos de acciones: 1) auditorías y 2) revisiones administrativas. Las revisiones administrativas las realizará el propio Comité con el apoyo de la Unidad de Transparencia, mientras que las auditorías las deberá realizar un actor externo al Comité de Transparencia, pudiendo ser: 1. Externas, cuando exista el presupuesto para ello y la importancia del caso lo amerite, o 2. Voluntarias, realizadas a través del Instituto de Transparencia conforme a lo que señala el artículo 170 de la Ley.

LA DEFINICIÓN DE ACCIONES PARA LA MEJORA CONTINUA.

El proceso de revisión y mejora continua permitirá verificar que los parámetros establecidos en la Ley, en los Lineamientos Generales, en este Programa de Protección de Datos Personales y en el Documento de Seguridad y demás normatividad aplicable de la que deriven obligaciones en materia de protección de Datos Personales se cumplan estrictamente o permitan realizar los ajustes necesarios para su cumplimiento y perfeccionamiento.

Con lo anterior se permitirá garantizar el tratamiento óptimo de los datos personales en posesión de la Fiscalía.

En ese sentido, la Unidad de Transparencia, por sí o a petición de las áreas, dará cuenta al Comité de Transparencia de los puntos de mejora en materia de protección de datos personales que hayan sido advertidos de las auditorías y/o revisiones internas realizadas, así como de aquellos eventos derivados del Documento de Seguridad para la Protección de Datos Personales de la Fiscalía; o bien, de aquellas circunstancias que se estimen relevantes o de inmediata aplicación para perfeccionar las directrices incluidas en este Programa.

El Comité de Transparencia por sí o a través de la Unidad de Transparencia realizará las recomendaciones que estime conveniente en materia de protección de datos personales, teniendo como finalidad fundamental que las unidades administrativas adopten acciones preventivas y correctivas, debiendo documentar los resultados y revisiones de los puntos de mejora desarrollados.

SANCIONES.

De manera enunciativa más no limitativa son causa de sanción de las obligaciones establecidas en la Ley, las señaladas en el artículo 188 de dicho ordenamiento Jurídico, el cual se cita para pronta referencia:

Artículo 188. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los Derechos ARCO;
II. Incumplir los plazos de atención previstos en la Ley para responder las solicitudes para el ejercicio de los Derechos ARCO o para hacer efectivo el derecho de que se trate;
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida Datos Personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
IV. Dar Tratamiento, de manera intencional, a los Datos Personales en contravención a los principios y deberes establecidos en la Ley;
V. No contar con el Aviso de Privacidad, o bien, omitir en el mismo alguno de los elementos a que refieren los artículos 38 y 39 de la Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;
VII. Incumplir el deber de confidencialidad establecido en el artículo 59 de la Ley;
VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 47, 48 y 50 de la Ley;
IX. Presentar vulneraciones a los Datos Personales por la falta de implementación de medidas de seguridad según los artículos 47, 48 y 50 de la Ley;
X. Llevar a cabo la Transferencia de Datos Personales, en contravención a lo previsto en la presente Ley;
XI. Obstruir los actos de verificación de la autoridad;
XII. Crear bases de Datos Personales en contravención a lo dispuesto por el artículo 9 de la Ley;
XIII. No acatar las resoluciones emitidas por el Instituto de Transparencia;
XIV. Aplicar medidas compensatorias en contravención de los criterios que tales fines establezca el Sistema Nacional;
XV. Declarar dolosamente la inexistencia de Datos Personales cuando éstos existan total o parcialmente en los archivos del Responsable;
XVI. No atender las medidas cautelares establecidas por el Instituto de Transparencia;
XVII. Tratar los Datos Personales de manera que afecte o impida el
ejercicio de los derechos fundamentales previstos en la Constitución Política de los Estados Unidos Mexicanos;
XVIII. No cumplir con las disposiciones previstas en los artículos 85, 90 y 91 de la Ley;
XIX. Tratar Datos Personales en aquellos casos en que sea necesario presentar la evaluación de impacto a la protección de Datos Personales, de conformidad con lo previsto en la Ley y demás normativa aplicable, y

XX. Realizar actos para intimidar o inhibir a los Titulares en el ejercicio de los Derechos ARCO.

Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, XV, XVI, XVIII, XIX y XX, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

En cuanto al procedimiento que se seguirá para que se determinen las sanciones en caso de incumplimiento a los supuestos referidos previamente, se estará a lo dispuesto en términos de la normatividad aplicable.

FISCALÍA GENERAL DEL ESTADO DE PUEBLA

DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES

2024

www.fiscalia.puebla.gob.mx /fiscaliapuebla @FiscaliaPuebla
Blvd. Héroes del 5 de Mayo y 31 Oriente, col. Ladrillera de Benítez
C.P. 72530, Puebla, Pue. (222) 211 79 00 Ext. 4019 y 4050

ÍNDICE

INTRODUCCIÓN.....3

I. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.....4

II. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.....7

III. ANÁLISIS DE RIESGOS.....8

IV. ANÁLISIS DE BRECHA.....9

V. PLAN DE TRABAJO.....10

VI. MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.....13

VII. PROGRAMA DE CAPACITACIÓN.....15

INTRODUCCIÓN

Tanto la Ley General de Transparencia y Acceso a la Información Pública, como la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, tienen por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier sujeto obligado, así como garantizar el acceso, rectificación, cancelación y oposición de datos personales por parte de sus titulares, garantizando su protección.

Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados define los datos personales como cualquier información concerniente a una persona física identificada o identificable, para lo que se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. Por otra parte, hace la distinción entre los datos personales sensibles, los cuales define como aquellos que se refieran a la esfera más íntima, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, para enunciar algunos se consideran sensibles los datos que revelan aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas o morales, así como las opiniones políticas o preferencia sexual, etc.

De conformidad con lo dispuesto en el artículo 1 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, es de observancia obligatoria en el Estado de Puebla y tiene por objeto garantizar el derecho que tiene toda persona a la protección de sus Datos Personales.

Para la consecución de su objeto, esta Fiscalía General cuenta con diversas atribuciones, en cuyo ejercicio tiene acceso al tratamiento de diversos datos personales, los cuales se distribuyen en sus respectivos sistemas de tratamientos.

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, establece dentro de sus deberes una serie de medidas de seguridad que los responsables deberán observar en la protección de datos personales, en este sentido, el artículo 51 de la citada Ley, prevén la obligación de elaborar un “documento de seguridad”.

Por lo anterior, la Fiscalía General del Estado de Puebla, con la finalidad de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, emite el presente documento, en observancia de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, con la intención de brindar homogeneidad en la organización y procesos para la protección de los datos personales.

Asimismo, el presente documento tiene como propósito controlar internamente el universo de datos personales en posesión del Instituto, el tipo de datos personales que contienen los archivos, los responsables, las obligaciones, el análisis de riesgos y los mecanismos de monitoreo y revisión de las medidas de seguridad, entre otros.

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

En cumplimiento a lo establecido en los artículos 33, fracción III y 35, fracción I de la Ley General de Datos Personales en Posesión de Sujetos Obligados y 51 de Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, la Fiscalía General del Estado, con la finalidad de establecer y mantener las medidas de seguridad para la protección de los datos personales, emitió el presente inventario de datos personales y de los sistemas de tratamiento, con la información básica del tratamiento de datos personales señalado por las Unidades Administrativas de este Órgano Autónomo.

1. OFICIALÍA MAYOR

1.1 Sistema de Registro de Acceso a las Instalaciones	
Finalidad del tratamiento	Registrar y mantener actualizada la información de las personas que ingresan a las instalaciones de la Fiscalía General.
Datos personales recabados	Nombre, foto, huella digital. (datos personales no sensibles).
Uso de los datos	Mantener un registro de las personas que ingresan a las instalaciones de la Fiscalía General.
Formato de almacenamiento	Electrónico (Base de datos en formato Excel).
Descripción general de ubicación física y/o electrónica	Carpeta compartida de la Oficialía Mayor, en los servidores de la Fiscalía General, únicamente personal facultado por la Oficialía Mayor cuenta con acceso a
Fundamento legal	De conformidad con Lineamientos L/014/2021 de Seguridad Institucional en las Instalaciones de la Fiscalia General del Estado de Puebla Artículos 5, fracciones VIII y XXXV, 14 y 16 de la
Cargo del servidor responsable	Oficial Mayor.

2. UNIDAD DE TRANSPARENCIA

2.1 Sistema de Registro de Solicitudes de Acceso a la Información y Solicitudes ARCO	
Finalidad del tratamiento	Registrar y mantener actualizada la información de las solicitudes que ingresan a través de la Plataforma Nacional de Transparencia y demás habilitados para ello.
Datos personales recabados	Nombre, correo electrónico, sexo. (datos personales no sensibles).
Uso de los datos	Mantener un registro de las solicitudes que son recibidas por la Fiscalía General.
Formato de almacenamiento	Electrónico (Base de datos en formato Excel).
Descripción general de ubicación física y/o electrónica	Carpeta compartida de la Unidad de Transparencia, en los servidores de la Fiscalía General, únicamente personal facultado por la Unidad de Transparencia
Fundamento legal	De conformidad con el articulo 187 fracción IV del Reglamento de la Ley Orgánica de la Fiscalía General del Estado. Artículos 5, fracciones VIII y XXXV, 14 y 16 de la
Cargo del servidor responsable	Titular de la Unidad de Transparencia.

3. COORDINACIÓN GENERAL DE ESTADÍSTICA Y SISTEMAS DE INFORMACIÓN

3.1 Sistema de Control y Evaluación de la Gestión Institucional	
Finalidad del tratamiento	Es una herramienta de inteligencia en procuración de justicia, útil para la toma de decisiones y para evaluar permanentemente la actividad sustantiva de la Institución.
Datos personales recabados	Nombre, sexo, fecha de nacimiento, dirección, teléfono, características fiscas. (datos personales sensibles).

Uso de los datos	El sistema permite llevar en tiempo real el control de la actividad sustantiva de la Institución, mediante el registro de la información relativa a las Carpetas de Investigación y su curso por cada una de las etapas del procedimiento penal.
Formato de almacenamiento	Electrónico (Base de datos).
Descripción general de ubicación física y/o electrónica de los datos personales	Sistema de gestión de la Coordinación General de Estadística y Sistemas de Información, en los servidores de la Fiscalía General, únicamente personal facultado por la Coordinación General de Estadística y Sistemas de Información cuenta con acceso a dicha sistema.
Fundamento legal	De conformidad con el artículo 144 del Reglamento de la Ley Orgánica de la Fiscalía General del Estado. Artículos 5, fracciones VIII y XXXV, 14 y 16 de la LPDPPSOEP.
Cargo del servidor responsable	Coordinadora General de Estadística y Sistemas de Información

II. Funciones y obligaciones de las personas que traten datos personales

De conformidad con el artículo 5, fracción XXXV de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, los servidores públicos de la Fiscalía General que traten datos personales en el ejercicio de sus funciones y de las atribuciones de la Unidad Administrativa a la que se encuentran adscritos observarán, al menos, las medidas de seguridad técnicas siguientes:

a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

Adicionalmente, los servidores públicos de la Fiscalía General, al tratar los datos personales, observarán las siguientes funciones y obligaciones:

Funciones:

- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- Llevar un registro de los servidores públicos que accedan a los datos personales y llevar a cabo las acciones necesarias para que sea necesaria la autenticación de los usuarios.
- Mantener actualizada la relación de usuarios que traten datos personales.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar dicho incidente a la Unidad de Transparencia de la Fiscalía General y llevar el registro de los hechos.

Obligaciones:

- Llevar a cabo permanentemente las medidas de seguridad de carácter administrativo, físico y técnico necesarias para la protección de los datos personales, evitando daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizando la confidencialidad, integridad y disponibilidad de los mismos.

Atender los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus atribuciones no se difundan, distribuyan o comercialicen.

III. Análisis de Riesgos

Los datos personales a los que los servidores públicos de la Fiscalía General tienen acceso en el ejercicio de sus atribuciones, se resguardan de manera física y electrónica, según las necesidades de la actividad para la cual se lleva a cabo su tratamiento.

Tanto para la protección de datos personales, como para los datos personales sensibles, determinados junto con su ciclo de vida por las Unidades Administrativas en el "Inventario de Datos Personales y de los Sistemas de Tratamiento" de la Fiscalía General observa el máximo nivel de protección; es decir, sin discriminarlos por su valor o ciclo de vida, pues su vulneración podría tener como consecuencia negativa para los titulares de los datos personales la divulgación o incluso un daño en su esfera más íntima, daño moral o patrimonial, entre otros, siendo que el valor de los datos personales en la actualidad cobra cada día mayor relevancia por las implicaciones e información vinculados a ellos.

En este sentido, tanto los sistemas electrónicos como los medios a través de los cuales se resguardan de manera física los datos personales presentan diferentes particularidades en razón de las características de cada uno de ellos.

Por lo que hace a los datos personales que se resguardan de manera física, los riesgos existentes son la pérdida o uso indebido de la información, deterioro negligente, así como su destrucción; por ello, la Fiscalía General cuenta con un área soporte encargada de ejecutar acciones para garantizar la seguridad de la información, manteniendo en un mínimo su exposición, pues únicamente pueden acceder a ellos los servidores públicos facultados y con acreditación para su uso.

Por su parte, los datos personales contenidos en un sistema electrónico presentan riesgos por su propia naturaleza como lo son el uso indebido de la información, la falla en los equipos electrónicos o en los sistemas; por ello, la Fiscalía General cuenta con un área soporte encargada de ejecutar acciones para garantizar la seguridad de la información, manteniendo en un mínimo su exposición, pues únicamente pueden acceder a ellos los servidores públicos facultados y previa acreditación de su personalidad a través de medios electrónicos para su uso.

IV. Análisis de brecha

Las medidas de seguridad existentes y efectivas para la protección de datos personales con las que actualmente cuenta la Fiscalía General, son las siguientes:

1. Medidas de seguridad: La información que contiene datos personales se resguarda en una ubicación que cuenta con diversas medidas de seguridad como cámaras de seguridad, archiveros específicos para su resguardo y uso de cerraduras para su acceso.
2. Medidas de control: Medidas de carácter administrativo encaminadas a contar con un registro físico de los servidores públicos que tienen acceso a datos personales, así como de los datos personales contenidos en los documentos.
3. Medidas legales: Cuando se lleva a cabo la transferencia de datos personales entre sujetos obligados o entre servidores públicos de la Fiscalía General, se realiza el apercibimiento en cuanto al trato que se le deberá dar a los mismos, en los términos de la legislación vigente en la materia.
4. Medidas cibernéticas: La Coordinación General de Estadística y Sistemas de Información, cuenta con atribuciones para establecer normas y lineamientos e implementar esquemas de seguridad para la infraestructura de tecnología de la información, comunicaciones y sistemas que permitan garantizar conexiones seguras, tanto al exterior como al interior de la Fiscalía General.

A efecto de fijar la brecha entre las medidas de seguridad con las que cuenta la Fiscalía General y las faltantes y/o nuevas por implementar, se han identificado las siguientes:

1. Implementar en los siguientes planes de capacitación de personal, nuevos cursos o programas enfocados a la protección de datos personales.
2. Designar a un responsable para la rendición de cuentas de la gestión de los datos personales, de modo que tanto el cumplimiento de la legislación en protección de datos personales, como la política de gestión y seguridad de datos personales, puedan ser demostrados.
3. El responsable designado para la protección de datos personales, deberá estar a cargo del cumplimiento de la política de protección de datos personales de manera cotidiana.
4. Implementar mecanismos o programas tecnológicos novedosos para garantizar las amenazas que se presenten en materia de ciberseguridad en el futuro.
5. Se deben designar deberes y obligaciones respecto a los servidores públicos que intervengan en el uso y protección de datos personales.

V. Plan de Trabajo

Atendiendo a lo dispuesto en el análisis de riesgo y el análisis de brecha desarrollado en el presente documento y con la intención de definir las acciones a implementar para garantizar la protección de datos personales, se formuló el plan de trabajo siguiente:

Acciones	Temporalidad	Responsable	Descripción
Medidas cotidianas de protección de datos personales			
Gestión de datos personales	Permanente	Usuario de los datos personales	Se respetarán las medidas implementadas para el mantenimiento de los diferentes controles establecidos para salvaguardar los datos personales relacionados durante su tratamiento.
Prevención del mal uso de activos informáticos	Permanente	Coordinación General de Estadística y Sistemas de Información	Se deben tener mecanismos contra el uso de activos para propósitos no autorizados, como son los sistemas electrónicos, la utilización de bloqueos en caso de que usuarios no autorizados traten de acceder a módulos que no tienen permitido.
Cumplimiento legal			
Identificación de legislación	Al momento de iniciar el	Usuario de los datos	Se identificarán los deberes y responsabilidades para

aplicable	tratamiento de datos personales	personales con auxilio de ser necesario de la Coordinación General de Asuntos Jurídicos	cumplir con los requerimientos legales relacionados con la protección de datos personales.
Actualización de registro de usuarios	Cada que se lleven a cabo modificaciones	Encargado del registro de cada Unidad Administrativa	Se deben mantener actualizados los registros de los usuarios de datos personales.

Acciones	Temporalidad	Responsable	Descripción
Comunicación permanente al momento de llevar a cabo transferencia de datos personales	Al momento de que se lleve a cabo la transferencia de datos personales	Los servidores públicos que realicen la transferencia	Cuando se lleva a cabo la transferencia de datos personales entre sujetos obligados o entre servidores públicos de la Fiscalía General, se realizará el apercibimiento en cuanto al trato que se le deberá dar a los mismos, en los términos de la legislación vigente en la materia.
Recomendaciones en materia de seguridad de la información	Al momento de identificarlas	Personal de la Unidad de Transparencia	Cuando sea adecuado, obtener el consejo y recomendaciones de un especialista en protección de datos y seguridad de la información.
Acompañamiento	Al momento de que acontezca una contingencia	Personal adscrito a la Unidad de Transparencia y a la Coordinación General de Asuntos Jurídicos	Se llevará a cabo el acompañamiento y asesoría del personal adscrito a la Unidad de Transparencia y a la Coordinación General de Asuntos Jurídicos al momento de llevar a cabo las acciones apropiadas en caso de un incidente o vulneración de seguridad.

Estructura organizacional			
Designación de deberes en seguridad y protección de datos personales	Al momento de identificarlas	Titulares de las Unidades Administrativas	Se deben designar deberes y obligaciones respecto a los servidores públicos que intervengan en el uso y protección de datos personales.
Contratos con proveedores	Permanente	Área contratante	En la elaboración de los contratos con proveedores, revisar las cláusulas referentes a los requerimientos de seguridad y de tratamiento de datos personales para verificar su correspondencia con los requerimientos de la Fiscalía General.
Seguridad del personal			
Capacitación	Anualmente	Unidad de Transparencia	Los servidores públicos de la Unidad de Transparencia privilegiarán la asesoría en materia de datos personales para los servidores públicos de la Fiscalía General, incluyéndolos en su plan anual de capacitación.
Resguardo de la documentación	Permanente	Usuario de los datos personales	Cualquier documento o activo de información crítico debe estar resguardado, fuera de la vista, cuando éste no sea atendido.

VI. Mecanismos de monitoreo y revisión de las medidas de seguridad

En el presente documento de seguridad para la protección de datos personales, se detallan las acciones que establecen el mantenimiento de las medidas de seguridad en las cuales de manera general se destaca que el objeto de las mismas es la protección de los datos personales.

Para ello, con la finalidad de mantener un monitoreo y revisión de las medidas de seguridad, se llevarán a cabo de manera permanente las acciones siguientes:

1. La Unidad de Transparencia llevará un monitoreo del cumplimiento por parte de los servidores públicos que intervengan en las actividades detalladas en el Plan de Trabajo del presente documento.
2. Se mantendrá actualizado el inventario de datos personales y de los sistemas de tratamiento de los mismos.
3. La Coordinación General de Estadística y Sistemas de Información, mantendrá monitoreados los esquemas de seguridad implementados para la infraestructura de tecnología de la información, comunicaciones y sistemas que permitan garantizar conexiones seguras, tanto al exterior como al interior del Instituto.
4. Para garantizar el cumplimiento de las políticas en materia de protección de datos personales establecidas en el presente documento de seguridad, el mismo se publicará en la Intranet Institucional de la Fiscalía General y se enviará por medios electrónicos a los servidores públicos de la Institución.
5. Se llevarán a cabo diversas medidas de seguridad físicas para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento mediante las siguientes actividades:
    - Prevenir el acceso no autorizado al perímetro del lugar en que se resguarden los datos personales en sus instalaciones físicas.
    - Prevenir el daño o interferencia a las instalaciones físicas, recursos e Información.
    - Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico, que pueda salir de las instalaciones de la organización.
    - Proveer a los equipos que contienen o almacenan datos personales de un
    - mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.
6. En relación con el monitoreo de la seguridad se observará lo dispuesto en el artículo 48 fracción VII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Puebla, el cual establece que deberá 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.

   En este sentido, las acciones a monitorear son las siguientes:

- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica entre otras.
- Las nuevas amenazas que podrían estar activadas dentro y fuera de la organización y que no han sido valoradas.
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas pasadas que vuelvan a surgir.
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

VII. Programa de capacitación

La Fiscalía General del Estado, ha promovido la capacitación de los servidores públicos en materia de protección de datos personales, mediante los Cursos de Formación Inicial, impartido por la Unidad de Transparencia, adquiriendo los conocimientos de los aspectos fundamentales de la Ley, con la finalidad de garantizar el derecho a la protección de los mismos.

En este sentido, se busca continuar con la promoción de la capacitación en la materia, a través de los cursos citados e incluir con el apoyo del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Puebla (ITAIPUE), nuevos cursos que permitan ampliar los conocimientos adquiridos por los servidores públicos de la Fiscalía General, por lo que se continuará en constante comunicación con el citado Instituto para tales efectos.

- Cronograma de capacitación

NÚMERO	UNIDAD ADMINISTRATIVAS
1	Fiscalía Especializada en Derechos Humanos
2	Fiscalía de Investigación Metropolitana
3	Fiscalía de Investigación Regional
4	Fiscalía Especializada en Investigación de los Delitos de Desaparición Forzada de Personas y Desaparición Cometida por Particulares
5	Fiscalía Especializada en Investigación de Secuestro y Extorsión
6	Fiscalía Especializada de Combate a la Corrupción
7	Fiscalía Especializada en Investigación de Delitos Electorales
8	Fiscalía Especializada en Investigación de Delitos de Alta Incidencia
9	Fiscalía Especializada en Investigación de Delitos de Violencia de Género contra las Mujeres
10	Fiscalía Especializada de Asuntos Internos
11	Fiscalía Especializada en Investigación del Delito de Tortura y otros Tratos Crueles, Inhumanos o Degradantes
12	Fiscalía Especializada en Investigación de los Delitos de Operaciones con Recursos de Procedencia Ilícita, Fiscales y Relacionados
13	Oficialía Mayor
14	Agencia Estatal de Investigación
15	Instituto de Ciencias Forenses
16	Órgano Interno de Control

17	Visitaduría General
18	Instituto de Formación Profesional
19	Coordinación General Especializada en Investigación de Robo de Vehículos
20	Coordinación General Especializada en Investigación de Homicidios Dolosos
21	Coordinación General de Mecanismos Alternativos de Solución de Controversias en Materia Penal
22	Coordinación General de Análisis de Información
23	Coordinación General de Colaboración Interinstitucional
24	Coordinación General de Estadística y Sistemas de Información
25	Coordinación General de Gestión Documental Institucional
26	Coordinación General de Asuntos Jurídicos
27	Coordinación General de Servicios a la Comunidad
28	Coordinación General de Investigación
29	Coordinación General de Litigación
30	Coordinación General de Desarrollo Institucional
31	Dirección General de Seguridad Institucional
32	Dirección General de Planeación Institucional
33	Dirección General de Comunicación Estratégica y Vinculación Social
34	Unidad Especializada en Materia de Extinción de Dominio
35	Unidad Especializada en Materia de Seguridad Vial

Noviembre						
Do	**Lu**	**Ma**	**Mi**	**Ju**	**Vi**	**Sa**
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Diciembre						
Do	**Lu**	**Ma**	**Mi**	**Ju**	**Vi**	**Sa**
1	2	3	4	5	6	7

8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				