



DOCUMENTO DE SEGURIDAD DE DATOS PERSONALES

De conformidad con lo establecido en los artículos 38, 40, 41, 42, de la Ley de Protección de Datos Personales el Posesión de Sujetos Obligados para el Estado de Colima, se emite el documento de seguridad que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas, adoptadas por la Secretaría de Planeación, Finanzas y Administración, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

I. Inventario de datos personales y de los sistemas de tratamiento

Se incorporan al presente instrumento el inventario de datos personales de los sistemas de tratamiento, correspondientes al semestre enero-junio de 2025.

(1) Nombre del Inventario (Se recomienda darle al inventario el nombre del área que lo gestiona, ejemplo: Inventario del área Administrativa, o de los datos que se recaban, ejemplo: Inventario de datos personales)	(2) Número de registros (Ejemplo: el inventario del área de asesorías a ciudadanos consta de 4 registros, porque en la asesoría se recaba: 1. Nombre, 2. Domicilio particular, 3. Teléfono y 4. Edad)	Inventario de datos personales			Sistema de tratamiento de datos personales Es el medio en que se encuentran contenidos y se da tratamiento a los datos personales que se mencionan en el inventario, FÍSICO (documentos y carpetas) o electrónico (base de datos)		
		(3) Fecha de implementación (Inicio aproximado cuando se originó el)	(4) Cambio SI/NO ¿Se han agregado o eliminado datos?	(5) Fecha de cambios (Aproximada)	(6) Fecha de implementación (Aproximada, si no se tiene el dato colocar NA)	(7) Cambio SI/NO ¿Se cambió la captura de los datos del medio físico a electrónico?	(8) Fecha de cambios (Aproximada, si no colocar NA)
Inventario de Datos Personales de la Dirección General de Recursos Humanos.	1. Nombre	N/A	N/A	N/A	2016	NO	N/A
	2. Estado Civil	N/A	N/A	N/A	2016	NO	N/A
	3. Registro Federal de Contribuyentes (RFC)	N/A	N/A	N/A	2016	NO	N/A
	4. Clave Única de Registro de Población (CURP)	N/A	N/A	N/A	2016	NO	N/A
	5. Lugar de nacimiento	N/A	N/A	N/A	2016	NO	N/A
	6. Fecha de nacimiento	N/A	N/A	N/A	2016	NO	N/A
	7. Nacionalidad	N/A	N/A	N/A	2016	NO	N/A
	8. Domicilio	N/A	N/A	N/A	2016	NO	N/A
	9. Teléfono particular	N/A	N/A	N/A	2016	NO	N/A
	10. Teléfono celular	N/A	N/A	N/A	2016	NO	N/A
	11. Sexo	N/A	N/A	N/A	2016	NO	N/A
	12. Correo electrónico	N/A	N/A	N/A	2016	NO	N/A
	13. Firma autógrafa	N/A	N/A	N/A	2016	NO	N/A
	14. Edad	N/A	N/A	N/A	2016	NO	N/A
	15. Fotografía	N/A	N/A	N/A	2016	NO	N/A
	16. Huellas dactilares	N/A	N/A	N/A	2016	NO	N/A
	17. Referencias personales	N/A	N/A	N/A	2016	NO	N/A
	18. Número de licencia de manejo	N/A	N/A	N/A	2016	NO	N/A
	19. Datos familiares	N/A	N/A	N/A	2016	NO	N/A
	Datos laborales	N/A	N/A	N/A	2016	NO	N/A



	20. Número de control	N/A	N/A	N/A	2016	NO	N/A
	21. Número de IMSS	N/A	N/A	N/A	2016	NO	N/A
	22. Puesto o cargo que desempeña	N/A	N/A	N/A	2016	NO	N/A
	23. Unidad de adscripción	N/A	N/A	N/A	2016	NO	N/A
	24. Teléfono institucional	N/A	N/A	N/A	2016	NO	N/A
	25. Antecedentes laborales	N/A	N/A	N/A	2016	NO	N/A
	26. Experiencia/Capacitación laboral	N/A	N/A	N/A	2016	NO	N/A
	27. Pertenencia a un sindicato	N/A	N/A	N/A	2016	NO	N/A
	Datos académicos	N/A	N/A	N/A	2016	NO	N/A
	28. Trayectoria educativa	N/A	N/A	N/A	2016	NO	N/A
	29. Nivel máximo de estudios	N/A	N/A	N/A	2016	NO	N/A
	30. Títulos, Cédula profesional	N/A	N/A	N/A	2016	NO	N/A
	31. Último comprobante de estudios	N/A	N/A	N/A	2016	NO	N/A
	32. Profesión	N/A	N/A	N/A	2016	NO	N/A
	33. Certificados	N/A	N/A	N/A	2016	NO	N/A
	Datos de salud	N/A	N/A	N/A	2016	NO	N/A
	34. Estado de salud físico	N/A	N/A	N/A	2016	NO	N/A
Inventario de Datos Personales de la Dirección General de Ingresos	Consta de 13 registros: 1. Nombre	2017	N/A	2020	2017	SI	2023
	2. RFC	2017	N/A	2020	2017	SI	2023
	3 CURP	2017	N/A	2020	2017	SI	2023
	4. Identificaciones oficiales	2017	N/A	2020	2017	SI	2023
	5. Domicilio particular	2017	N/A	2020	2017	SI	2023
	6. Nacionalidad	2017	N/A	2020	2017	SI	2023
	7. Ocupación	2017	N/A	2020	2017	SI	2023
	8. Teléfono	2017	N/A	2020	2017	SI	2023
	9. Correo electrónico	2017	N/A	2020	2017	SI	2023
	10. Declaraciones fiscales	2017	N/A	2020	2017	SI	2023
	11. Número de cuentas bancarias	2017	N/A	2020	2017	SI	2023
	12. Actividad económica	2017	N/A	2020	2017	SI	2023
	13. Datos vehiculares	2017	N/A	2020	2017	SI	2023
Inventario de datos que se recaban en el proceso de evaluación de ingreso del Sistema de Profesionalización.	1. Nombre	N/A	NO	N/A	N/A	NO	N/A
	2. Edad	N/A	NO	N/A	N/A	NO	N/A
	3. CURP	N/A	NO	N/A	N/A	NO	N/A
	4. Sexo	N/A	NO	N/A	N/A	NO	N/A
	5. Firma autógrafa	N/A	NO	N/A	N/A	NO	N/A



	6. Registro Federal de Contribuyentes	N/A	NO	N/A	N/A	NO	N/A
	7. Domicilio particular	N/A	NO	N/A	N/A	NO	N/A
	8. Número telefónico	N/A	NO	N/A	N/A	NO	N/A
	9. correo electrónico	N/A	NO	N/A	N/A	NO	N/A
	10. Referencias personales	N/A	NO	N/A	N/A	NO	N/A
	11. Antecedentes laborales	N/A	NO	N/A	N/A	NO	N/A
	12. Grado académico	N/A	NO	N/A	N/A	NO	N/A
	13. Trayectoria educativa	N/A	NO	N/A	N/A	NO	N/A
Inventario de datos que se recaban en el proceso de evaluación de desarrollo del Sistema de Profesionalización	1. nombre	N/A	NO	N/A	N/A	NO	N/A
	2. Edad	N/A	NO	N/A	N/A	NO	N/A
	3. Sexo	N/A	NO	N/A	N/A	NO	N/A
	4. Número de control	N/A	NO	N/A	N/A	NO	N/A
	5. Dependencia en la que labora	N/A	NO	N/A	N/A	NO	N/A
	6. Número de teléfono particular	N/A	NO	N/A	N/A	NO	N/A
	7. Correo electrónico	N/A	NO	N/A	N/A	NO	N/A
	8. Grado académico	N/A	NO	N/A	N/A	NO	N/A
Inventario de datos que se recaban en el proceso de evaluación de competencias del Sistema de Profesionalización	1. Nombre	N/A	NO	N/A	N/A	NO	N/A
	2. Puesto funcional	N/A	NO	N/A	N/A	NO	N/A
	3. Dependencia en que labora	N/A	NO	N/A	N/A	NO	N/A
	4. Número de control	N/A	NO	N/A	N/A	NO	N/A
	5. Correo electrónico	N/A	NO	N/A	N/A	NO	N/A
	6. Número telefónico particular	N/A	NO	N/A	N/A	NO	N/A
Inventario de datos que se recaban en el proceso de capacitación del Sistema de Profesionalización.	1. Nombre del participante	2021	NO	N/A	2021	NO	N/A
	2. Número de control	2021	NO	N/A	2021	NO	N/A
	3. Correo electrónico	2021	NO	N/A	2021	NO	N/A
	4. Número de teléfono particular	2021	NO	N/A	2021	NO	N/A
Inventario de usuarios de sistemas y servicios web	1. Nombre	2024	NO	N/A	2024	NO	N/A

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

De conformidad con lo establecido en el artículo 4, fracciones XXI y XXII, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Colima, los servidores públicos de la Secretaría de Planeación, Finanzas y Administración, que traten datos personales en el ejercicio de sus funciones y de las atribuciones de la unidad administrativa a la que encuentren adscritos, observarán, al menos, las medidas de seguridad siguientes:



1. Prevenir el acceso no autorizado al perímetro de la unidad administrativa, sus instalaciones físicas, áreas críticas, recursos e información;
2. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la unidad administrativa, recursos e información;
3. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la unidad administrativa;
4. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.
5. Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
6. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
7. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware;
8. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Adicionalmente, los servidores públicos de la Secretaría de Planeación, Finanzas y Administración, al tratar datos personales, observarán las siguientes funciones y obligaciones:

- a) Resguardar los datos personales a los que tenga acceso en el ejercicio de sus atribuciones
- b) Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos se encuentren actualizados
- c) Llevar un registro de los servidores públicos que accedan a los datos personales y llevar a cabo las acciones necesarias para la autenticación de los usuarios
- d) Mantener actualizada la relación de usuarios que traten datos personales
- e) En caso de presentarse algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, deberán informarlo a la Unidad de Transparencia de la Secretaría de Planeación, Finanzas y Administración
- f) 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 garantizar la confidencialidad, integridad y disponibilidad de los mismos.
- g) 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.
- h) Cumplir con la normatividad de la Ley de Protección de Datos Personales, garantizando la seguridad y confidencialidad de los datos.
- i) Llevar a cabo las medidas de seguridad administrativas, técnicas y físicas para proteger los datos contra accesos no autorizados, pérdida, alteración o destrucción.
- j) Responder a las solicitudes de derechos ARCO de forma eficiente y oportuna.
- k) Actuar con transparencia y responsabilidad, asegurando que los datos sean exactos, completos, correctos y actualizados.
- l) Proteger los datos contra accesos no autorizados, pérdida, alteración o destrucción y respetar la privacidad de los titulares.
- m) Informar a los titulares sobre el tratamiento de sus datos mediante el aviso de privacidad, especificando las características principales del mismo, para que puedan tomar decisiones informadas.
- n) Cumplir con todas las disposiciones legales en materia de protección de datos personales.
- o) Mantener la seguridad de los datos personales durante en ejercicio de las funciones del puesto.
- p) Respetar la privacidad del titular, obteniendo su consentimiento para el tratamiento de sus datos.

- q) No tratar los datos de forma engañosa o fraudulenta y tratar los datos de forma transparente y honesta, evitando cualquier manipulación.
- r) Mantener los datos personales completos, correctos y actualizados.
- s) Tramitar las consultas, solicitudes y reclamos relacionados con el tratamiento de los datos.
- t) No transferir datos personales salvo aquellas estrictamente necesarias para atender requerimientos de información de diversas autoridades fiscales, de seguridad social, fiscalizadoras, investigadoras, judiciales y administrativas.
- u) Documentar roles y responsabilidades de las personas que tratan datos personales, así como la cadena de rendición de cuentas, según el sistema de gestión implementado. Esto incluye la identificación de los perfiles de puesto y la definición de las responsabilidades de cada persona.
- v) Poner a disposición del titular de los datos personales el aviso de privacidad previo iniciar el uso de los datos personales para la finalidad para la que se obtuvieron.
- w) Ubicar el aviso de privacidad en un lugar visible, que facilite su consulta, con independencia del medio de difusión o reproducción que se utilice.
- x) Notificar oportunamente cualquier incidente de seguridad.

III. Análisis de riesgos

Los datos personales a los que los servidores públicos de la Secretaría de Planeación, Finanzas y Administración 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.

Para la protección de datos personales, la Secretaría de Planeación, Finanzas y Administración 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.

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 Secretaría de Planeación, Finanzas y Administración, cuenta con un área de archivo, 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.

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 Secretaría de Planeación, Finanzas y Administración, cuenta con un área de tecnologías, 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 los usuarios y contraseñas, previamente otorgados.

Algunos de los riesgos a los que la Secretaría de Planeación, Finanzas y Administración se encuentra expuesta en el resguardo de los datos personales son los siguientes:

- a) El acceso no autorizado a bases de datos donde se almacenan datos personales pueden comprometer la confidencialidad y disponibilidad de la información.
- b) El rastreo de la actividad online de las personas permite recopilar información personal si su consentimiento, que puede ser utilizada para fines maliciosos.

- c) El acceso no autorizado a sistemas informáticos puede permitir a otras personas no autorizadas a obtener datos personales, comprometer la privacidad y dañar la reputación.
- d) La manipulación indebida de los datos personales, como la divulgación no autorizada o el uso incorrecto, puede tener consecuencias negativas para los titulares.
- e) La pérdida o destrucción de datos personales, ya sea accidental o deliberada.
- f) Las violaciones de datos personales y el uso indebido de información personal pueden generar sanciones legales y regulatorias.
- g) El uso de contraseñas fáciles de adivinar o reutilizadas en diferentes plataformas aumenta el riesgo de acceso no autorizado a los datos personales.

IV. Análisis de brecha

Las medidas de seguridad existentes y efectivas para la protección de datos personales con las que cuenta actualmente la Secretaría de Planeación, Finanzas y Administración, son las siguientes:

- Medidas de seguridad: la información que contiene datos personales se resguarda en una ubicación que cuenta con diversas medidas de seguridad, como cámaras, archiveros específicos para su resguardo y uso de cerraduras para su acceso.
- 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 los datos personales contenidos en los documentos.
- Medidas legales: Cuando se lleva a cabo la transferencia de datos personales entre sujetos obligados o entre servidores públicos de la Secretaría de planeación, Finanzas y Administración, se realiza previa solicitud debidamente fundada y motivada y se hace del conocimiento en cuanto al trato que se deberá dar a los mismos, en los términos de la legislación aplicable.
- Medidas cibernéticas: La Dirección General de Tecnologías de la Información y Comunicación, cuenta con atribuciones para establecer normas y lineamientos e implementar esquemas de seguridad para la infraestructura tecnológica, que permitan garantizar conexiones seguras, tanto al exterior como al interior, de la Secretaría de Planeación, Finanzas y Administración.

A efecto de fijar la brecha entre las medidas de seguridad con las que cuenta la Secretaría de Planeación, Finanzas y Administración 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 al Oficial de Protección de Datos Personales
3. Implementar mecanismos o programas tecnológicos novedosos para garantizar las amenazas que se presenten en materia de ciberseguridad en el futuro.
4. Contraseñas seguras y complejas, así como cambiarlas regularmente.
5. Actualizar periódicamente el acceso a los usuarios autorizados.
6. Realizar respaldos periódicos de los datos personales, para recuperación en caso de pérdida o daño.
7. Elaborar lineamientos formales para entregar o trasladar información de trabajadores a los titulares o coordinadores administrativos de las Dependencias, para asegurar el correcto manejo de datos personales y la responsabilidad compartida en su tratamiento.

V. Plan de trabajo

Debido a la importancia y el contexto actual en materia de datos personales, se debe mantener actualizado el plan de trabajo, el cual permita alcanzar los objetivos del sistema de seguridad de protección de datos personales.

Para la ejecución del presente documento de seguridad, se realizará las siguientes actividades:

- Se comunicará a los encargados, responsables y titulares de las unidades administrativas, de la Secretaría de Planeación, Finanzas y Administración, sobre la emisión del documento de seguridad, solicitando su apoyo para la difusión interna del mismo.
- El Comité de Transparencia revisará en coordinación con las unidades administrativas, el cumplimiento de las medidas, controles y acciones previstas en este documento.
- La actualización de las medidas de Seguridad para la protección de datos personales.
- Se emitirá un programa anual de capacitaciones y además se promoverá que el personal de este Sujeto Obligado se mantenga capacitado, no sólo por sus áreas internas, sino también mediante su asistencia a capacitaciones otorgadas por organismos competentes en la materia.

Respecto al 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 siguiente plan de trabajo:

1.- Medidas cotidianas de protección de datos personales.

ACCIONES	TEMPORALIDAD	RESPONSABLE	DESCRIPCIÓN
Gestión de datos personales	Permanente	Usuario de los datos personales	Respetar las medidas implementadas para el mantenimiento de los diferentes controles establecidos para salvaguardar los datos personales durante su tratamiento.
Prevención del mal uso de activos informáticos	Permanente	Usuario de los datos personales	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.

2.- Cumplimiento legal.

ACCIONES	TEMPORALIDAD	RESPONSABLE	DESCRIPCIÓN
Identificar la legislación aplicable	Al momento de iniciar el tratamiento de datos personales	Usuario de datos personales	Identificar los deberes y responsabilidades para cumplir con los requerimientos legales relacionados con la protección de datos personales.
Actualizar el registro de usuarios	Cada que se lleven a cabo modificaciones	Encargado de actualizar	Actualizar los registros de los usuarios de datos personales.
Comunicación al momento de llevar a cabo transferencia de datos personales	En el momento de transferir los datos personales	Los servidores públicos que realicen la Transferencia de los datos personales	Se realizará el apercibimiento en cuanto al trato que se deberá de dar al momento de realizar la transferencia de datos personales, en los términos de la legislación vigente.
Recomendaciones en materia de seguridad de la información	En el momento de identificarlas	Los servidores públicos	Cuando sea adecuado, obtener el consejo y recomendaciones de un especialista en protección de datos y seguridad de la información.



Acompañamiento	En el momento en el que se presente una contingencia	Los servidores públicos	Se llevará a cabo el acompañamiento y asesoría de los servidores públicos, al momento de llevar a cabo las acciones apropiadas en caso de un incidente o vulneración de seguridad.
----------------	--	-------------------------	--

3.- Estructura organizacional.

ACCIONES	TEMPORALIDAD	RESPONSABLE	DESCRIPCIÓN
Designar deberes en seguridad y protección de datos personales	Al momento de identificar	Titulares de las Unidades Administrativas	Designar deberes y obligaciones respecto a los servidores públicos que intervengan en el uso y protección de datos personales.

4.- Seguridad del personal.

ACCIONES	TEMPORALIDAD	RESPONSABLE	DESCRIPCIÓN
Capacitación	Anualmente	Los servidores públicos	Los servidores públicos recibirán una capacitación anual que deberá estar incluída en su plan anual de capacitación en materia de datos personales.
Resguardo de la documentación	Permanente	Los servidores públicos	Los documentos o archivo de información crítica debe estar resguardado, fuera de la vista, cuando este no sea atendido.

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

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

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.
2. Se mantendrá actualizado el inventario de datos personales y de los sistemas de tratamiento de los mismos.
3. La Dirección General de Tecnologías de la Información y Comunicación mantendrá monitoreados los esquemas de seguridad implementados para la infraestructura tecnológica, que permita garantizar conexiones seguras, tanto al exterior como en el interior de la Secretaría de Planeación, Finanzas y Administración.
4. Para garantizar el cumplimiento de las políticas en materia de protección de datos personales establecidas en el presente documentos, el mismo será publicado en el Portal de Transparencia de la Secretaría de Planeación, Finanzas y Administración y se enviará a los servidores públicos que integran cada unidad administrativa, a través de su enlace con la Unidad de Transparencia.
5. Se llevarán a cabo diversas medidas de seguridad físicas para proteger el entorno 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
 - Prevenir el daño o interferencia a las instalaciones, recursos e información que contenga datos personales
 - Proteger los recursos móviles y cualquier soporte físico o electrónico que pueda salir de las instalaciones de la Secretaría de Planeación, Finanzas y Administración
 - Proveer a los equipos que contienen o almacenan datos personales, de un mantenimiento eficaz que asegure su disponibilidad, funcionalidad e integridad.



- Proteger los documentos físicos, conforme al desarrollo de las tareas que desempeñan o a las funciones que se les encomiendan.

6. Serán monitoreadas las siguientes acciones:

- La migración tecnológica.
- La transferencia de información entre sujetos obligados y entre servidores públicos de la propia Secretaría de Planeación, Finanzas y Administración.
- Establecer medidas para limitar el acceso a los datos personales a personas autorizadas.
- Verificar las políticas y procedimientos de protección de datos personales se estén aplicando correctamente.
- Configurar las cuentas y perfiles con contraseñas robustas y cambiarlas frecuentemente.

VII. El programa general de capacitación.

Para que los servidores públicos lleven a cabo un manejo adecuado en la protección de datos personales, deben adquirir los conocimientos adecuados para garantizar el derecho a la protección de los mismos, se sugieren las siguientes temáticas:

- Principios y obligaciones en materia de protección de datos personales.
- Identificación y gestión de incidentes de seguridad.
- Buenas prácticas para el manejo seguro de información digital y física.
- Curso en relación a la “Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y sus Lineamientos”.

VIII. Mecanismos de restauración y/o recuperación de los datos personales en caso de destrucción o pérdida.

La Secretaría de Planeación, Finanzas y Administración, posee datos personales en sistemas electrónicos y físicos, por lo que, en caso de destrucción o pérdida, siempre es posible recuperarlos, pues la copia física también se encuentra en electrónico, además, se ha planteado en las diversas unidades administrativas de esta Dependencia, la posibilidad contar con el equipo necesario para realizar copias de seguridad de los datos personales, sin embargo, aún se encuentra en trámite.

EL TEMPLO DEL BRAZO ES
VIGOR EN LA TIERRA