RECOMENDACIONES en materia de seguridad de datos personales.

Al margen un sello con el Escudo Nacional, que dice: Estados Unidos Mexicanos.- Instituto Federal de Acceso a la Información y Protección de Datos.

El Pleno del Instituto Federal de Acceso a la Información y Protección de Datos, con fundamento en lo dispuesto por los artículos 19, 39, fracción IV de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; 58 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; 15, fracciones I y XXI, 24, fracción III, y 30, fracción II del Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos, y

CONSIDERANDO

Que uno de los deberes que rigen la protección de los datos personales es la implementación de medidas de seguridad para la protección de la información que está en posesión de los responsables y encargados del tratamiento de los datos personales;

Que en ese sentido, el artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece la obligación para todo responsable que lleve a cabo el tratamiento de datos personales, de implementar y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado de los mismos;

Que el Capítulo III del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares define de manera general los factores que deberán tomar en cuenta los responsables y encargados del tratamiento de datos personales para determinar las medidas de seguridad a implementar para la protección de los mismos, así como las acciones que deberán llevar a cabo los responsables y encargados para la implementación de las medidas de seguridad;

Que en los casos en que ocurra una vulneración a la seguridad de los datos personales, el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI o Instituto), en su caso, podrá tomar en consideración el cumplimiento de sus recomendaciones, para efectos del artículo 58 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;

Que, además de lo anterior, las recomendaciones del Instituto servirán de orientación a los particulares para determinar los procedimientos y mecanismos a aplicar para la seguridad de los datos personales;

Que de conformidad con el artículo 39, fracciones IV y V de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, el IFAI tiene las atribuciones de emitir recomendaciones para efectos de funcionamiento y operación de esa ley, así como para divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información; emite las presentes:

RECOMENDACIONES EN MATERIA DE SEGURIDAD DE DATOS PERSONALES

1. RECOMENDACIÓN GENERAL

El artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante, la Ley) establece que:

Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

Por su parte, el Capítulo III del Reglamento de la Ley detalla los factores y acciones que deben tomar en cuenta los responsables y encargados del tratamiento de datos personales para determinar las medidas de seguridad aplicables a la información personal que esté en su posesión.

Asimismo, el Instituto, en su caso, podrá tomar en consideración el cumplimiento de sus recomendaciones para efectos del artículo 58 del Reglamento de la Ley.

En ese sentido, y en ejercicio de la facultad que la fracción IV del artículo 39 de la Ley otorga al Instituto para emitir criterios y recomendaciones para el funcionamiento y operación de la Ley; el IFAI emite las presentes recomendaciones, a fin de que los responsables y encargados tengan un marco de referencia respecto de las acciones que se consideran como las mínimas necesarias para la seguridad de los datos personales.

RECOMENDACIÓN GENERAL

Para la seguridad de los datos personales, el IFAI RECOMIENDA la adopción de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP), basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar).

Es importante que se tome en cuenta que el alcance del SGSDP es la protección de los datos personales y su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Por lo cual, el análisis de riesgos y las medidas de seguridad implementadas como resultado del seguimiento de las presentes recomendaciones, se deberán enfocar en la protección de datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, así como en evitar las vulneraciones descritas en el artículo 63 del Reglamento de la Ley.

Estas recomendaciones se basan en la seguridad a través de la gestión del riesgo de los datos personales, entendiéndose de forma general al riesgo como una combinación de la probabilidad de que un incidente ocurra y de sus consecuencias desfavorables; de modo tal

que al determinar el riesgo en un escenario específico de la organización, se pueda evaluar el impacto y realizar un estimado de las medidas de seguridad necesarias para preservar la información personal.

Es importante señalar que la adopción de las presentes recomendaciones es de carácter voluntario, por lo que los responsables y encargados podrán decidir libremente qué metodología conviene más aplicar en su negocio para la seguridad de los datos personales. Asimismo, el seguimiento de las presentes recomendaciones no exime a los responsables y encargados de su responsabilidad con relación a cualquier vulneración que pudiera ocurrir a sus bases de datos, ya que la seguridad de dichas bases depende de una correcta implementación de las medidas o controles de seguridad.

A continuación se explica lo que en estas recomendaciones se entiende por Sistema de Gestión de Seguridad de Datos Personales, y las acciones mínimas a considerar para su implementación.

2. SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

2.1 Conceptos clave

Activo. La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización.

Alta Dirección. Toda persona con poder legal de toma de decisión en las políticas de la organización. Por ejemplo: la junta directiva, ejecutivos y trabajadores experimentados, la persona a cargo del departamento de datos personales, los socios de la organización, el dueño de una empresa unipersonal o quien encabeza la organización.

Datos personales. Cualquier información concerniente a una persona física identificada o identificable.

Datos personales sensibles. Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Encargado. La persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Impacto. Una medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

Incidente. Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.

- **Amenaza.** Circunstancia o evento con la capacidad de causar daño a una organización.

- **Vulnerabilidad.** Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Organización. Conjunto de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones.

Responsable. Persona física o moral de carácter privado que decide sobre el tratamiento de los datos personales.

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

Riesgo de seguridad. Potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización.

Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

- **Confidencialidad.** Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no autorizados.

- **Disponibilidad.** Propiedad de un activo para ser accesible y utilizable cuando lo requiera una entidad autorizada.

- **Integridad.** La propiedad de salvaguardar la exactitud y completitud de los activos.

Sistema de Gestión de Seguridad de Datos Personales (SGSDP). Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley, su Reglamento, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

Titular. La persona física a quien corresponden los datos personales.

Tratamiento. La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

2.2 Sistema de Gestión

La **gestión** es un conjunto de actividades coordinadas para dirigir y controlar un proceso o tarea. Un **sistema** es un conjunto de elementos mutuamente relacionados o que interactúan por un fin u objetivo. Por lo tanto, un **Sistema de Gestión (SG)** se define como un conjunto de elementos y actividades interrelacionadas para establecer **metas** y los **medios de acción** para alcanzarlas.

Asimismo, un sistema de gestión apoya a las organizaciones en la dirección, operación y control de forma sistemática y transparente de sus procesos, a fin de lograr con éxito sus actividades, ya que está diseñado para mejorar continuamente el desempeño de la organización, mediante la consideración de las necesidades de todas las partes interesadas.

Es importante tomar en cuenta que una organización tiene que definir y gestionar numerosas actividades para funcionar con eficiencia. Estas actividades se convierten en procesos que tienen la característica de recibir elementos de entrada, los cuales se gestionan para regresar al final de su ciclo, como elementos de salida (resultados). Por ejemplo, un proceso de Auditoría puede recibir como elementos de entrada objetivo, alcance y plan de auditoría, así como el informe de resultados de la auditoría anterior, y como elemento de salida un nuevo informe de auditoría. A menudo, la salida de un proceso se convierte directamente en la entrada del proceso siguiente, y la interconexión entre procesos genera sistemas que se retroalimentan para mejorar.

En el caso de las presentes recomendaciones, el sistema de gestión propuesto se basa en el modelo denominado "Planificar-Hacer-Verificar-Actuar" (PHVA), a través del cual se dirigen y controlan los procesos o tareas, como se puede ver en la tabla 1 y figura 1:

	Elemento del SG	Fase del PHVA	Actividades
PROCESO	**Metas**	**P**lanificar	Se identifican políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por la organización (meta).
	Medios de acción	**H**acer	Se implementan y operan las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
		Verificar	Se evalúan y miden los resultados de las políticas, objetivos, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.
		Actuar	Se adoptan medidas correctivas y preventivas, en función de los resultados y de la revisión, o de otras fuentes de información relevantes, para lograr la mejora continua.

Tabla 1. Sistema de Gestión

Figura 1. Ciclo General del Sistema de Gestión de Seguridad de Datos Personales

El SGSDP tiene como objetivo proveer un marco de trabajo para el tratamiento de datos personales, que permita mantener vigente y mejorar el cumplimiento de la legislación sobre protección de datos personales y fomentar las buenas prácticas.

Las fases del ciclo PHVA considera diferentes pasos y objetivos específicos para el SGSDP, que pueden observarse en la siguiente tabla:

Ciclo	**Fases**	**Pasos**	**Objetivos Específicos**
Planificar	Planear el SGSDP	1. Alcance y objetivos 2. Política de gestión de datos personales. 3. Funciones y obligaciones de quienes traten datos personales 4. Inventario de datos personales.	Definir los objetivos, políticas, procesos y procedimientos relevantes del SGSDP para **gestionar los riesgos de los datos personales**, con el fin de **cumplir con la legislación sobre protección de datos** y obtener resultados acordes con las políticas y objetivos generales de la organización.

		5. Análisis de riesgos de los datos personales. 6. Identificación de las medidas de seguridad y análisis de brecha.	
Hacer	Implementar y operar el SGSDP	7. Implementación de las medidas de seguridad aplicables a los datos personales.	Implementar y operar las políticas, objetivos, procesos, procedimientos y controles o mecanismos del SGSDP, considerando indicadores de medición.
Verificar	Monitorear y revisar el SGSDP	8. Revisiones y auditoría.	Evaluar y medir el cumplimiento del proceso de acuerdo con la **legislación de protección de datos personales**, la política, los objetivos y la experiencia práctica del SGSDP, e informar los resultados a la Alta Dirección para su revisión.
Actuar	Mejorar el SGSDP	9. Mejora continua y Capacitación.	Para lograr la mejora continua se deben adoptar medidas correctivas y preventivas, en función de los resultados obtenidos de la revisión por parte de la Alta Dirección, las auditorías al SGSDP y de la comparación con otras fuentes de información relevantes, como actualizaciones regulatorias, riesgos e impactos organizacionales, entre otros. Adicionalmente, se debe considerar la capacitación del personal.

Tabla 2. Objetivos del SGSDP dentro de las fases del ciclo PHVA

La mayoría de las organizaciones poseen uno o más procesos que involucran el tratamiento de datos personales; estos procesos deben ser identificados y controlados a partir de que la información es recolectada y hasta que se bloquea, se borra o destruye.

Más aún, en el marco de la Ley y su Reglamento, los datos personales son el principal activo de información. En consecuencia, a través del artículo 61 del Reglamento se puede vislumbrar que una de las primeras acciones para llevar a cabo su protección es tener bien identificado, definido y documentado el flujo de los datos personales que se traten a través de los diferentes procesos de la organización.

Asimismo, durante el ciclo del SGSDP se deben identificar los riesgos relacionados a los datos personales, así como al resto de activos que interactúan directamente con ellos, y de ese modo determinar los controles de seguridad que pueden mitigar los incidentes.

3. ACCIONES A IMPLEMENTAR PARA LA SEGURIDAD DE LOS DATOS PERSONALES

Las acciones mínimas a realizar en el Sistema de Gestión de Seguridad de Datos Personales son las siguientes:

FASE 1. PLANEAR EL SGSDP

PASO 1. **Alcance y Objetivos.** Consideraciones respecto al tratamiento de datos personales y el modelo de negocios de la organización.

PASO 2. **Política de Gestión de Datos Personales.** El compromiso formal documentado de la Alta Gerencia hacia el tratamiento adecuado de datos personales en la organización.

PASO 3. **Funciones y Obligaciones de Quienes Traten Datos Personales.** Asignación de responsabilidades para la implementación del SGSDP.

PASO 4. **Inventario de Datos Personales.** Identificación de los tipos de datos y su flujo.

PASO 5. **Análisis de Riesgo de los Datos Personales.**

- **Factores para Determinar las Medidas de Seguridad.** Conjunto de consideraciones que las organizaciones deben plantear como directrices para tratar el riesgo en función de sus alcances y objetivos.

- **Valoración Respecto al Riesgo.** Proceso de ponderación para identificar los escenarios de riesgo prioritarios y darles tratamiento proporcional.

PASO 6. **Identificación de las Medidas de Seguridad y Análisis de Brecha.** Proceso de evaluación de las medidas de seguridad que ya existen en la organización contra las que sería conveniente tener. Los controles de seguridad, sin que sean limitativos, deben considerar los siguientes dominios:

- Políticas del SGSDP
- Cumplimiento legal
- Estructura organizacional de la seguridad
- Clasificación y acceso de los activos
- Seguridad del personal
- Seguridad física y ambiental

- Gestión de comunicaciones y operaciones
- Control de acceso
- Desarrollo y mantenimiento de sistemas
- Vulneraciones de seguridad

FASE 2. IMPLEMENTAR Y OPERAR EL SGSDP

PASO 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.

· **Cumplimiento Cotidiano de Medidas de Seguridad.** Consideraciones para el trabajo cotidiano con datos personales, así como el plan de tratamiento del riesgo de los activos relacionados a los mismos.

· **Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.** Proceso en el que se decide y se implementa el tratamiento adecuado para un riesgo o grupo de riesgos respecto al contexto de la organización.

FASE 3. MONITOREAR Y REVISAR EL SGSDP

PASO 8. Revisiones y Auditoría. Proceso de revisión del funcionamiento del SGSDP respecto a la política establecida, cada vez que exista un cambio en el contexto del alcance y objetivos del SGSDP.

· **Revisión de los Factores de Riesgo.** Consideraciones para monitorear el estado del riesgo y aplicar las modificaciones pertinentes para mejorar el SGSDP.

· **Auditoría.** Requerimientos para los procesos de auditoría interna/externa.

· **Vulneraciones a la Seguridad de la Información.** Consideraciones en caso de un incidente de seguridad.

·

FASE 4. MEJORAR EL SGSDP

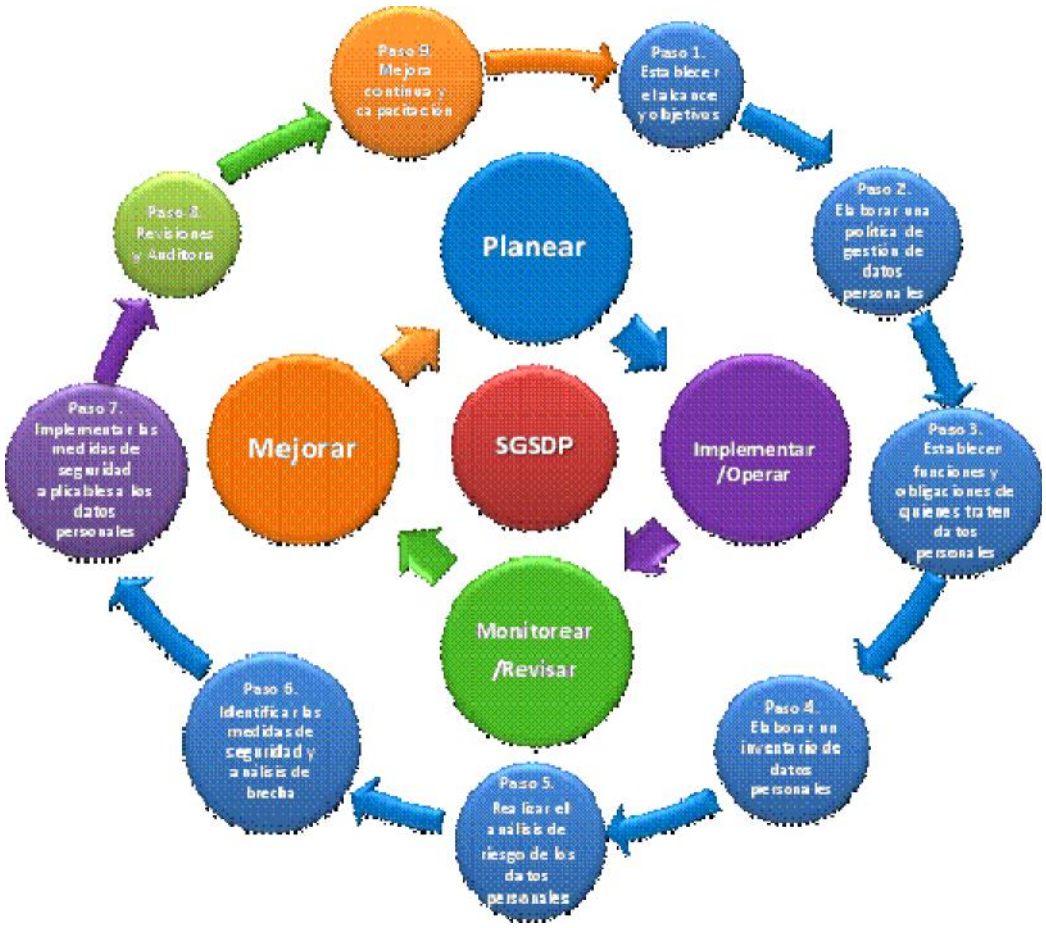
PASO 9. Mejora Continua y Capacitación. Consideraciones para incluir la protección de datos en la cultura de la organización y mantener siempre actualizado el SGSDP.

· **Mejora Continua.** La aplicación de medidas preventivas y correctivas sobre el SGSDP.

· **Capacitación.** Programas de mejora en la capacitación al personal

para mantener la vigencia del SGSDP.

La siguiente imagen muestra gráficamente el ciclo de estas acciones:



Para la implementación de estas acciones y en general del Sistema de Gestión de Seguridad de Datos Personales, el IFAI recomienda la consulta de los siguientes estándares internacionales, en los que se basan las Recomendaciones:

- BS 10012:2009, Data protection–Specification for a personal information management system.
- ISO/IEC 27001:2005, Information Technology–Security techniques–Information security management systems –Requirements.
- ISO/IEC 27002:2005, Information Technology–Security techniques–Code of practice for security management.
- ISO/IEC 27005:2008, Information Technology–Security techniques–Information security risk management.
- ISO/IEC 29100:2011, Information technology–Security techniques–Privacy framework.

- ISO 31000:2009, Risk management–Principles and guidelines.
- ISO GUIDE 72, Guidelines for the justification and development of management systems standards.
- ISO GUIDE 73, Risk management–Vocabulary.
- ISO 9000:2005, Quality management systems–Fundamentals and vocabulary.
- NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.
- OECD Guidelines for the Security of Information Systems and Networks–Towards a Culture of Security.

Por último, a continuación se ofrece un cuadro de análisis que permite comparar cuáles de estas acciones ayudan a cumplir con las obligaciones que establece el Capítulo III del Reglamento de la Ley:

Tabla Comparativa entre el Capítulo III del Reglamento de la Ley y las Recomendaciones

Capítulo III **De las Medidas de Seguridad en el Tratamiento de Datos Personales**	**Recomendación que ayuda a cumplir con la disposición**
Alcance	
Artículo 57. El responsable y, en su caso, el encargado deberán establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Capítulo, con independencia del sistema de tratamiento. Se entenderá por medidas de seguridad para los efectos del presente Capítulo, el control o grupo de controles de seguridad para proteger los datos personales. Lo anterior sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular que la dispuesta en la Ley y el presente Reglamento.	· Recomendación General. · Paso 1. Alcance y Objetivos. · Paso 2. Política de Gestión de Datos Personales.
Atenuación de Sanciones	
Artículo 58. En términos de lo dispuesto en el artículo 65, fracción III de la Ley, en los casos en que ocurra una vulneración a la seguridad de los datos personales, el Instituto podrá tomar en consideración el cumplimiento de sus recomendaciones para determinar la atenuación de la sanción que corresponda.	· Recomendación General.
Funciones de seguridad	
Artículo 59. Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.	· Paso 3. Funciones y Obligaciones de Quienes Traten Datos Personales. Asignación de responsabilidades para la implementación del SGSDP. · Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.

	o Cumplimiento Cotidiano de Medidas de Seguridad.
Factores para determinar las medidas de seguridad	
Artículo 60. El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores: **Fracción I** El riesgo inherente por tipo de dato personal; **Fracción II** La sensibilidad de los datos personales tratados; **Fracción III**. El desarrollo tecnológico, y **Fracción IV.** Las posibles consecuencias de una vulneración para los titulares. De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos: I. El número de titulares; II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.	· Paso 5. Realizar el Análisis de Riesgo de los Datos Personales. o Factores para Determinar las Medidas de Seguridad.
Acciones para la seguridad de los datos personales	
Artículo 61. A fin de establecer y mantener la seguridad de los datos personales, el responsable deberá considerar las siguientes acciones:	· Recomendación general.
Fracción I. Elaborar un inventario de datos personales y de los sistemas de tratamiento;	· Paso 4. Elaborar un Inventario de Datos Personales.

Fracción II. Determinar las funciones y obligaciones de las personas que traten datos personales;	· Paso 3. Establecer Funciones y Obligaciones de Quienes Traten Datos Personales.
Fracción III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales**;**	· Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.
Fracción IV. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;	· Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha. · Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.
Fracción V. Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;	· Paso 6. Identificación de las medidas de seguridad y Análisis de Brecha.
Fracción VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;	· Paso 7. Implementación de las Medidas de Seguridad Aplicables a los Datos Personales. o Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.
Fracción VII. Llevar a cabo revisiones o auditorías;	· Paso 8. Revisiones y Auditoría.
Fracción VIII. Capacitar al personal que efectúe el tratamiento, y	· Paso 9. Mejora Continua y Capacitación. o Capacitación.
Fracción IX. Realizar un registro de los medios de almacenamiento de los datos personales.	· Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.
El responsable deberá contar con una relación de las medidas de seguridad derivadas de las fracciones anteriores.	· Acciones a implementar para la seguridad de los datos personales documentadas.
Actualizaciones de las medidas de seguridad	
Artículo 62. Los responsables deberán actualizar la relación de las medidas de seguridad, cuando ocurran los siguientes eventos:	· Paso 8. Revisiones y Auditoría.

I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable; **II.** Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo; **III.** Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 del presente Reglamento, o **IV.** Exista una afectación a los datos personales distinta a las anteriores. En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.	
Vulneraciones de seguridad	
Artículo 63. Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase de tratamiento son: **I.** La pérdida o destrucción no autorizada; **II.** El robo, extravío o copia no autorizada; **III.** El uso, acceso o tratamiento no autorizado, o **IV.** El daño, la alteración o modificación no autorizada.	· Paso 5. Realizar el Análisis de Riesgo de los Datos Personales.
Notificación de vulneraciones de seguridad	
Artículo 64. El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin	· Paso 9. Mejora Continua y Capacitación. o Vulneraciones a la Seguridad de la Información.

dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.	
Información mínima al titular en caso de vulneraciones de seguridad	
Artículo 65. El responsable deberá informar al titular al menos lo siguiente: **I.** La naturaleza del incidente; **II.** Los datos personales comprometidos; **III.** Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses; **IV.** Las acciones correctivas realizadas de forma inmediata, y **V.** Los medios donde puede obtener más información al respecto.	· Paso 9. Mejora Continua y Capacitación. o Vulneraciones a la Seguridad de la Información.
Medidas correctivas en caso de vulneraciones de seguridad	
Artículo 66. En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.	· Paso 9. Mejora Continua y Capacitación. o Mejora Continua.

Así lo acordó el Pleno del Instituto Federal de Acceso a la Información y Protección de Datos, en sesión celebrada el día veintitrés del mes de octubre del año dos mil trece, ante el Secretario de Protección de Datos Personales.- El Comisionado Presidente, **Gerardo Laveaga Rendón**.- Rúbrica.- Los Comisionados: **Sigrid Arzt Colunga**, **Jacqueline Peschard Mariscal**, **María Elena Pérez-Jaén Zermeño** y **Ángel Trinidad Zaldívar**.- Rúbricas.- El Secretario de Protección de Datos Personales, **Alfonso Oñate Laborde**.- Rúbrica.**(R.- 378152)**