TOOLKIT DE CONCIENTIZACIÓN DE SEGURIDAD DE DATOS PERSONALES PARA RESPONSABLES DEL SECTOR PRIVADO

MÓDULO 1. Seguridad de datos personales

Índice

Seguridad de la información

a) Conceptos[1]

- **Seguridad de la información:** Protección de la información y de los sistemas de información contra el acceso, el uso, la divulgación, la interrupción, la modificación o la destrucción no autorizados con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

- **Seguridad informática:** Disciplina que involucra técnicas, aplicaciones y dispositivos que aseguran la autenticidad, integridad y privacidad de la información contenida en un sistema informático, así como durante su transmisión.

- **Ciberseguridad**: Es el conjunto de herramientas, políticas, conceptos, acciones, prácticas y tecnologías que se utilizan para garantizar la integridad, la confidencialidad o la disponibilidad de un sistema o una red de información, protegiendo al mismo tiempo a las y los usuarios y sus dispositivos de los riesgos de seguridad que hay en el ciberentorno.

- **Ciberentorno:** Incluye a usuarios, redes, dispositivos, todo el software, procesos, información almacenada o que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a las redes. Las instalaciones y edificios donde residen los dispositivos también forman parte del ciberentorno.[2]

- **Vulneraciones:** De acuerdo con el artículo 63 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[3], las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:

    - La pérdida o destrucción no autorizada.
    - El robo, extravío o copia no autorizada.
    - El uso, acceso o tratamiento no autorizado.
    - El daño, la alteración o modificación no autorizada.

[1] Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/

[2] Disponible en: https://blog.nivel4.com/noticias/mes-nacional-de-la-ciberseguridad-pero-que-es-la-ciberseguridad/

[3] Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

b) Elementos de la seguridad de la información

La seguridad de la información tiene como finalidad esencial resguardar y proteger la información, preservando en todo momento los siguientes principios[4]:

- **Confidencialidad:** Asegurar que la información no se ponga a disposición o se divulgue a personas, entidades o procesos no autorizados.

Ejemplo:
- Otorgar acceso a la información solamente a las personas autorizadas, proporcionándoles un usuario y una contraseña.

- **Disponibilidad:** Asegurar que la información sea accesible y utilizable a petición de una entidad autorizada.

Ejemplo:
- Garantizar que los datos personales que se tratan en los sistemas informáticos de la organización puedan ser consultados cuando sea requerido.

- **Integridad:** Asegurar que la información no ha sido alterada sin la autorización correspondiente.

Ejemplo:
- Establecer restricciones en los sistemas de información para evitar que usuarios sin autorización realicen cambios en los datos personales tratados en dichos medios.

[4] Disponible en: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/

- **Autenticación:** Verificar la identidad de un individuo, dispositivo o proceso para tener acceso a la información.

Ejemplo:
- La autenticación de los empleados de la organización para brindar el acceso a zonas restringidas se puede realizar, por ejemplo, mediante el uso de una contraseña o un rasgo biométrico (voz, retina, iris).

- **Control de acceso:** Medios para garantizar que el acceso a los activos esté autorizado y restringido en función de los requisitos de la empresa y de la seguridad.

Ejemplo:
- Entregar una tarjeta de identificación electrónica para tener acceso al inmueble o al espacio específico en el que se almacena la información.

- **No repudio:** Capacidad para corroborar la autoría de un mensaje o información, evitando que el autor niegue la existencia de su recepción o creación.

Ejemplo:
- Envío de información únicamente desde el correo institucional.

c) Retos de la seguridad de la información

El desarrollo vertiginoso de las tecnologías de la información y la comunicación (TIC), así como el aumento exponencial de los usuarios de internet y de dispositivos móviles, conlleva el surgimiento de retos que, de no atenderse de manera oportuna y conjunta, pueden poner en riesgo a las personas titulares de los datos, así como a los responsables del tratamiento.

A continuación, se enlistan, de manera enunciativa más no limitativa, algunos retos identificados:

- Ataques a dispositivos físicos interconectados a través de redes inalámbricas (Internet de las Cosas [5]IoT.
- Ataques a las cadenas de bloques y a las criptomonedas[6].
- Ataques de *phishing*[7].
- Ataques *ransomware*[8].
- Ciberataques[9].
- Riesgos a la seguridad en la nube.
- Uso de la inteligencia artificial para realizar ataques en la red.

[5] El **Internet de las cosas** (en inglés, Internet of things, abreviado IoT; IdC, por sus siglas en español) es un concepto que se refiere a una interconexión digital de objetos cotidianos con internet.
[6] La **criptomoneda**, también llamada moneda virtual o criptodivisa, es dinero digital. Eso significa que no hay monedas ni billetes físicos — todo es en línea.
[7] **Phishing** es un término informático que distingue a un conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza haciéndose pasar por una persona, empresa o servicio de confianza (suplantación de identidad de tercero de confianza), para manipularla y hacer que realice acciones que no debería realizar (por ejemplo revelar información confidencial o hacer click en un enlace).
[8] Un **ransomware** (del inglés ransom, «rescate», y ware, acortamiento de software), o «secuestro de datos» en español, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.
[9] Un **ciberataque** es un intento malicioso y deliberado por parte de un individuo o una organización para irrumpir en el sistema de información de otro individuo u otra organización.

Seguridad de datos personales

a) Deber de seguridad en la LFPDPPP

La **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)**, **concretamente el artículo 19**, establece que todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad para proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Las medidas de seguridad se clasifican y definen, de conformidad con el **Reglamento de la LFPDPPP**, de la siguiente manera:

- **Administrativas (Art. 2 fracción V):** Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales.

Ejemplos:

- Desarrollar e implementar políticas, procedimientos y mejores prácticas internas y externas.
- Implementar contraseñas, claves y protocolos de seguridad.
- Elaborar planes de trabajo y medidas de monitoreo y revisión.
- Desarrollar programas de capacitación de personal.
- Emisión de reglas sobre la instalación, uso y conexión de equipos electrónicos y de cómputo que se utilizan para el tratamiento de la información.

- **Físicas (Art. 2 fracción VI):** Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para:
    - Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información.

- Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones.
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad.
- Garantizar la eliminación de datos de forma segura.

Ejemplos:
- Proteger las instalaciones, equipos, soportes y bases de información.
- Instalar sistemas de vigilancia y alarmas.
- Instalar dispositivos de identificación que requieran datos biométricos para ingresar a las instalaciones.

- **Técnicas (Art. 2 fracción VII):** Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:

  - El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados.
  - El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.
  - Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros.
  - Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

Ejemplos:
- Recurrir a técnicas de encriptación y cifrado de la información, así como de disociación y seudonimización.
- Realizar respaldos de la información.
- Dar mantenimiento a los equipos electrónicos y de cómputo y actualizar constantemente los sistemas.
- Instalar firewalls, antivirus y otros mecanismos para evitar la pérdida y filtración de la información.

b) Factores para determinar las medidas de seguridad

De acuerdo con el artículo 60 del Reglamento de la LFPDPPP, los responsables determinarán las medidas de seguridad que aplicarán al interior de su organización considerando, al menos, los siguientes factores:

- El desarrollo tecnológico.
- El número de personas titulares.
- El riesgo inherente por tipo de dato personal.
- 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.
- La sensibilidad de los datos personales tratados.
- Las posibles consecuencias de una vulneración para las personas titulares.
- Las vulnerabilidades previas ocurridas en los sistemas de tratamiento.

Además, se deberán considerar otros factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

c) Actualizaciones de las medidas de seguridad

El artículo 62 del Reglamento de la LFPDPPP establece que los responsables deberán actualizar la relación de las medidas de seguridad cuando ocurran los siguientes eventos:

- Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable.
- Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo.
- Se vulneren los sistemas de tratamiento.
- Exista una afectación a los datos personales distinta a las anteriores.

Además, se establece que, al tratarse de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.

Obligaciones de los responsables con el deber de seguridad

a) Cómo cumplir con el deber de seguridad

De conformidad con el **Reglamento de la LFPDPPP**, el responsable deberá considerar las siguientes acciones para establecer y mantener la seguridad de los datos personales.

- **Política de gestión de datos personales (Art. 48, fracción I):** Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable que incluyan, como mínimo, los siguientes elementos:

    - Alcance y objetivos de la política.
    - Cumplimiento con los principios y deberes establecidos en la LFPDPPP, en su Reglamento y en la demás normatividad aplicable.
    - Excepciones consideradas en la normativa aplicable.
    - Partes interesadas y miembros responsables del tratamiento de datos personales.
    - Clasificación y tipo de datos personales.
    - Ciclo de vida de los datos personales.
    - Obligaciones y responsabilidades.
    - Aprobación del área correspondiente.
    - Medios para su difusión y conocimiento.
    - Mecanismos para evaluar su efectividad.
    - Sanciones en caso de incumplimiento.

    Esta política deberá ser comunicada a todos los miembros que participen con el responsable o el Encargado.

- **Inventario de datos personales (Art. 61, fracción I):** Un registro actualizado de los sistemas de tratamiento de datos personales que utiliza una organización. En dicho registro se deben

identificar la información básica que permita conocer el tipo de tratamiento al que son sometidos los datos personales, la cual se relaciona de manera directa con su flujo o ciclo de vida (recolección, uso, almacenamiento, divulgación, bloqueo y cancelación). Además, es indispensable identificar, entre otros elementos, la categoría de datos personales, los soportes (físicos y/o electrónicos) que se utilizan para su tratamiento y el tipo de tratamiento realiza cada miembro de la organización.

Ejemplo:

Sistema de tratamiento	Finalidades	Tipo o categoría de datos personales	Personal involucrado	Encargados	Terceros	Difusión	Plazo de conservación

- **Análisis de riesgo de los datos personales (Art. 61, fracción III):** El proceso de análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad.

  El análisis de riesgo se puede realizar de diversas formas; sin embargo, se recomienda la metodología BBA (**B**eneficio para el atacante; **A**ccesibilidad para el atacante; **A**nonimidad del atacante), la cual se enfoca en tres variables que afectan la percepción del valor de los datos personales para un atacante.

  A continuación, se explican las variables referidas.

  - **Beneficio:** factor que contempla el nivel de riesgo inherente del dato según su tipo y el volumen de personas titulares de las que se tratan datos.
  - **Accesibilidad:** determinar la cantidad de accesos potenciales a los datos personales que se pretende

proteger, es decir, definir cuántas personas tienen la posibilidad de acceder a la información en un intervalo de tiempo. Para este parámetro, entre mayor sea la accesibilidad, mayor riesgo existe para la información.

- **Anonimidad:** definir qué tan anónimos son los accesos a la información; es decir, el nivel de riesgo por tipo de entorno (físico, red interna, red inalámbrica, red de terceros e internet). Es preciso recordar que entre más anónimo pueda ser un atacante, mayor confianza obtiene para intentar vulnerar la seguridad.
  Este factor representa el nivel de percepción que se tiene de que un atacante potencial provoque consecuencias negativas para la organización en caso de acceder o hacer uso no autorizado de los datos personales que se tratan.

La combinación de las tres variables da como resultado el nivel de riesgo latente que presenta cada organización. Posteriormente, se podrán identificar las medidas de seguridad aplicables a la organización.

Para más información, se sugiere consultar la **Metodología de Análisis de Riesgo BAA** publicada por el INAI.

Asimismo, se sugiere revisar estándares internacionales sobre la gestión de riesgos como ISO 31000 (Gestión de riesgos) e ISO 27005 (Gestión de riesgos de la Seguridad la Información).

- **Análisis de brecha (Art. 61, fracción V):** Es un análisis que consiste en identificar las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales. Para realizar este análisis se pueden seguir los siguientes pasos:

  - Identificar las medidas de seguridad que se implementan en la organización.
  - Evaluar la eficacia de dichas medidas.
  - Mejorar las medidas vigentes e identificar nuevas medidas a partir de mejores prácticas, estándares, guías y recomendaciones.

- Elaborar un plan de acción para la eventual implementación de las medidas identificadas que incluya tiempos, responsables, procedimientos y demás contenido necesario.

Una vez identificadas las medidas de seguridad faltantes, es recomendable establecer un plan de trabajo para su eventual implementación.

Para realizar este análisis se sugiere consultar el **Evaluador de vulneraciones** y el **anexo D (Ejemplos de controles de seguridad) de la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales**. Además, existen estándares internacionales como la ISO 27001 (Seguridad de la información) e ISO 27701 (Gestión de la privacidad de la información) que pueden aportar elementos útiles al análisis de brecha.

- **Revisiones y auditorías (Art. 61, fracción VII y Art. 48, fracción III):** Las organizaciones deben establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de las políticas de privacidad (revisiones), así como su eficacia y eficiencia (auditoría objetiva e imparcial), incluyendo, para el caso específico de la gestión de seguridad de datos personales, el monitoreo de los siguientes puntos:

  - Nuevos activos que se incluyan en los alcances de la gestión de riesgo.
  - Modificaciones necesarias a los activos, por ejemplo, cambio o migración tecnológica.
  - Nuevas amenazas que podrían estar activas 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.
  - Vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelven a surgir.
  - Cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.

- Incidentes y vulneraciones de seguridad.

Lo anterior, permitirá conocer el valor de los activos, las amenazas, vulnerabilidades, el impacto, y la probabilidad de ocurrencia de vulneraciones, para identificar en una etapa temprana cualquier suceso que requiera una atención específica.

Es importante aclarar que el riesgo no es estadístico, es decir, las amenazas, vulnerabilidades, probabilidad y consecuencias pueden cambiar abruptamente sin previo aviso, por lo que se requiere la revisión de cada riesgo por separado, así como la suma de ellos, para conocer el impacto potencial acumulado de las amenazas. Esto implica un monitoreo sistémico para detectar esos cambios, para lo cual se puede recurrir a servicios externos que provean información respecto a las amenazas o vulnerabilidades.

- **Programas de capacitación interna (Art. 61, fracción VIII):** Brindar al personal de la organización información actualizada sobre sus responsabilidades y deberes respecto a la protección de datos personales, incluyendo, como mínimo, los siguientes rubros:

  - Requerimientos y actualizaciones al contexto del SGSDP.
  - Legislación en materia de protección de datos personales.
  - Mejores prácticas aplicables a la organización.
  - Consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales.
  - Herramientas tecnológicas utilizadas para el tratamiento de datos personales y para la implementación de medidas de seguridad.

  Como parte de los programas, es indispensable desarrollar pruebas teóricas y/o prácticas para evaluar el grado de conocimiento y/o entendimiento de la capacitación proporcionada. Por ende, es necesario establecer criterios de evaluación que determinen el nivel de competencia aceptado por la organización, y mantener un registro de los programas seguidos por cada empleado, así como de sus habilidades, experiencia y calificaciones.

Por último, los programas pueden adquirir diferente modalidad en función de su alcance y objetivo, a saber:

- **Concienciación:** programas a corto plazo para la difusión en general de la protección de datos personales en la organización.
- **Entrenamiento:** programas a mediano plazo que tienen por objetivo capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales.
- **Educación:** programa general a largo plazo que tiene por objetivo incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de la organización.

b) Sistema de Gestión de Seguridad de Datos Personales

En las Recomendaciones en materia de Seguridad de Datos Personales, publicadas en el Diario Oficial de la Federación el 30 de octubre de 2013, el INAI recomendó la implementación de un Sistema de Gestión de Seguridad de Datos Personales (SGSDP) basado en el ciclo PHVA (Planear-Hacer-Verificar-Actuar), para la protección de los datos personales, mismo que se describirá más adelante.

De acuerdo con la **Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales** publicada por el INAI, un Sistema de Gestión de Seguridad de Datos Personales (SGSDP) se puede definir como un 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 LFPDPPP, su Reglamento, normatividad secundaria y cualquier otro principio que la buena práctica internacional estipule en la materia.

Si bien existen diferentes modelos para diseñar e implementar un sistema de gestión y, de este modo, establecer metas y los medios de acción para alcanzarlas, se recomienda el denominado "Planificar-Hacer-Verificar-Actuar" (PHVA) o Ciclo Deming, nombrado así en

honor a su creador (William Edwards Deming). Este proceso es el más utilizado por las empresas para realizar actividades de mejora continua en sus respectivas actividades y, con ello, mejorar sus niveles de rendimiento y productividad.

En el caso específico del SGSDP, se contemplan los siguientes pasos y objetivos específicos para cada una de las fases:

Fase		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 **5.** Análisis de riesgos de los datos personales **6.** Identificación de las medidas de seguridad y análisis de brecha	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.
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 y procedimientos del SGSDP, así como sus controles o mecanismos con 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.

Como se puede advertir en el cuadro anterior, el diseño e implementación del SGSDP consiste básicamente en seguir los nueve pasos en estricto orden. **Para más información, se sugiere consultar la sección 3. Acciones para la Seguridad de los Datos Personales de la**

"Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales" publicada por el INAI.

c) Esquemas de autorregulación

De acuerdo con la **Guía de Esquemas de Autorregulación en Materia de Protección de Datos Personales** publicada por el INAI, la autorregulación es la posibilidad que tienen los responsables y encargados de establecer y autoimponerse voluntariamente reglas para el debido tratamiento de datos personales que complementen lo previsto por la normativa, elevando los estándares de protección de ésta y considerando las particularidades de los responsables o encargados que desarrollan y adoptan esta clase de reglas. Sirven para adecuar y armonizar las disposiciones contenidas en las normas aplicables a la realidad de sectores u organizaciones específicos.

La incorporación de un esquema de autorregulación como parte de las medidas de protección de datos personales se encuentra prevista en **el artículo 44 de la LFPDPPP y en los artículos 47, 79 a 86 de su Reglamento**. Dicha incorporación conlleva diversos beneficios para las organizaciones, sobre todo en un mercado altamente competitivo en el que cada vez más los consumidores cuidan el uso y destino de su información personal.

Los esquemas de autorregulación pueden adoptar los siguientes formatos:

- **Reglas emitidas con objeto de adaptar la normativa** aplicable en materia de protección de datos personales a la realidad y actividades de un sector en particular.
- **Esquemas con validación**, total[10] o parcial[11] en función de los principios, deberes y obligaciones previstos en la normativa correspondiente. Estos son evaluados y validados por el INAI cuando satisfagan los requisitos previstos para ello.
- **Esquemas con certificación reconocida**, total o parcial en función de los principios, deberes y obligaciones previstos en la

[10] Cuando se establezcan con relación a todos los principios, deberes y obligaciones previstos en la Ley, el Reglamento, los Parámetros y demás normativa aplicable en la materia.
[11] Cuando se establezcan con relación a principios, deberes y obligaciones específicos previstos en la Ley, el Reglamento, los Parámetros y demás normativa aplicable en la materia.

normativa correspondiente. Estos esquemas son certificados por un organismo de certificación en materia de datos personales.
- **Esquemas desarrollados y reconocidos fuera del territorio mexicano**, respecto de los cuales el INAI puede desarrollar un estudio de equivalencia considerando la normativa mexicana.

En cuanto al contenido de los esquemas, estos deben contemplar, como mínimo, los siguientes elementos:

- Especificación de la denominación del esquema de autorregulación.
- Especificación del nombre completo, denominación o razón social de los responsables o encargados adheridos al esquema.
- Especificación del sector o actividad a la que aplica el esquema (por ejemplo, si aplica al sector automotriz, bancario, hospitalario).
- Descripción del alcance del esquema, es decir, si es total o parcial y si aplica a todos o a algunos tratamientos que realiza el adherido o adheridos.
- Descripción del ámbito personal de aplicación, es decir, el tipo o grupo de personas titulares cuyos datos personales están vinculados con el tratamiento al que aplica el esquema de autorregulación (por ejemplo, clientes, empleados, visitantes, etcétera).
- Desarrollar un Sistema de Gestión de Datos Personales (SGDP), el cual se describe de manera general en el siguiente apartado.
- Documentarse y desarrollarse en idioma español.
- Datos de contacto o un medio habilitado para que los interesados conozcan más acerca del esquema.

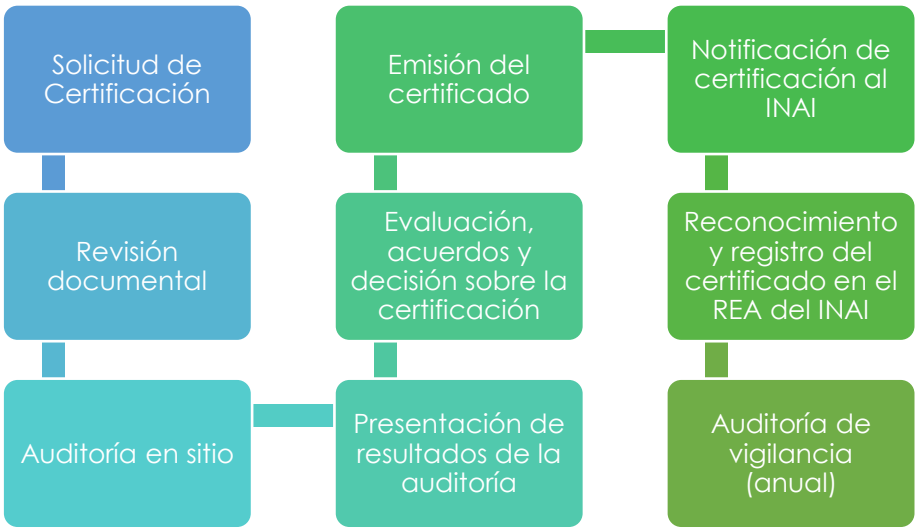
Además de los elementos referidos, los responsables o encargados pueden incluir en sus esquemas de autorregulación los siguientes contenidos potestativos:

- Mecanismos alternativos de solución de controversias.
- Algún distintivo que identifique a responsables o encargados adheridos a esquemas con validación o certificación reconocida, adicional al que el Instituto pudiere prever como consecuencia del reconocimiento o validación correspondiente.

- Disposiciones relativas al alcance y vinculación internacional del esquema.

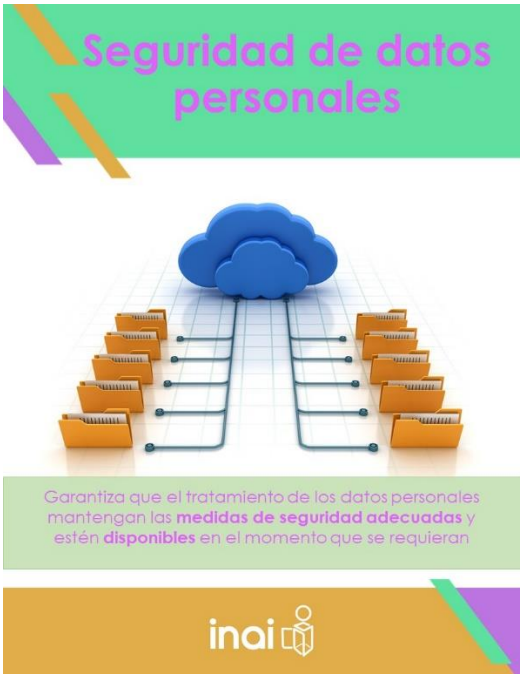
Finalmente, es importante aclarar que los esquemas de autorregulación deben someterse a una certificación en materia de protección de datos personales, con una vigencia de 2 años, que tiene por objeto que las personas acreditadas como organismos de certificación determinen la conformidad o grado de cumplimiento de los esquemas, y de su implementación, así como prácticas y herramientas tecnológicas que adopten los responsables y encargados con relación a la Ley, su Reglamento, los Parámetros de Autorregulación y demás normativa aplicable a la materia, así como de estándares y mejores prácticas que decidan adoptar.

En cuanto al procedimiento para la acreditación de un esquema de autorregulación, a continuación, se presenta un esquema sobre dicho proceso:



Para más información, se sugiere consultar los **Parámetros de Autorregulación en materia de Protección de Datos Personales**, así como la **Guía de Esquemas de Autorregulación en materia de Protección de Datos Personales** que publicó el INAI.

Materiales de difusión




¿Extraviaste tu tarjeta de acceso?
Usa tus **tarjetas de acceso y contraseñas** con responsabilidad, en caso de extravío repórtalo de inmediato
inai


¿Utilizas canales seguros de comunicación?
Email
19
Envía información y/o datos personales únicamente desde el **correo corporativo o medios seguros designados** para este fin
inai


Revisa los perfiles y privilegios en los sistemas de tratamiento
Verifica de forma periódica **los permisos del personal** que trata datos personales en tu organización
inai


Medidas de seguridad
Consulta la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y su Reglamento para conocer las **medidas de seguridad que se pueden implementar para proteger los datos personales**, así como las obligaciones que deberás observar para cumplir con el **deber de seguridad** de los datos personales
¡Cumple con las medidas de seguridad de tu organización!
inai

Artículos de interés

- Evaluador de vulneraciones.
- Guía de Esquemas de Autorregulación en materia de Protección de Datos Personales.
- Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales.
- ISO 27001 (Seguridad de la información).
- ISO 27005 (Gestión de riesgos de la Seguridad la Información).
- ISO 27701 (Gestión de la privacidad de la información).
- ISO 31000 (Gestión de riesgos).
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).
- Metodología de Análisis de Riesgo BAA.
- Parámetros de Autorregulación en materia de Protección de Datos Personales.
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Examen de evaluación

1. **¿Qué normativa regula la protección de datos personales en el sector privado?**

   a) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
   b) Ley Federal de Telecomunicaciones
   c) Ley Federal de Protección de Datos Personales en Posesión de los Particulares
   d) Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales
   e) Ninguna de las anteriores

2. **¿Cuáles son las vulneraciones de datos?**

   a) La pérdida o destrucción no autorizada
   b) El robo, extravío o copia no autorizada
   c) El uso, acceso o tratamiento no autorizado
   d) El daño, la alteración o modificación no autorizada
   e) Todas las anteriores

3. **¿La seguridad de la información tiene como finalidad esencial resguardar y proteger la información, preservando en todo momento los principios de confidencialidad, disponibilidad, integridad, autenticación, control de acceso, no repudio?**

   a) Verdadero
   b) Falso

4. **¿Cuál es el objetivo principal de las medidas de seguridad que debe establecer y mantener todo responsable que lleve a cabo tratamiento de datos personales?**

   a) Proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado
   b) Garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (Derechos ARCO)
   c) Ayudar a los empleados con la realización de sus actividades

d) Fomentar la confianza de los clientes

5. **¿Cuál es la clasificación de las medidas de seguridad para proteger los datos personales?**

a) Administrativas y técnicas
b) Digitales y físicas
c) Económicas y sociales
d) Administrativas, físicas y técnicas
e) Públicas y privadas

6. **¿Cuáles son los pasos para realizar un análisis de brecha?**

a) Identificar las medidas de seguridad que se implementan en la organización
b) Evaluar la eficacia de dichas medidas
c) Mejorar las medidas vigentes e identificar nuevas medidas a partir de mejores prácticas, estándares, guías y recomendaciones
d) Elaborar un plan de acción para la eventual implementación de las medidas identificadas que incluya tiempos, responsables, procedimientos y demás contenido necesario
e) Todas las anteriores

7. **La siguiente frase es verdadera o falsa: "Las organizaciones deben establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de las políticas de privacidad (revisiones), así como su eficacia y eficiencia (auditoría objetiva e imparcial)"**

a) Verdadera
b) Falsa

8. **Un Sistema de Gestión de Seguridad de Datos Personales es:**

a) Un programa informático para proteger los dispositivos de cualquier sistema malicioso o *malware*

b) Un sistema de seguridad físico para proteger los dispositivos en los que se almacenan la información, incluyendo los datos personales
c) Un sistema para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales
d) Un sistema de alerta para las vulneraciones de datos personales
e) Ninguna de las anteriores

9. Los esquemas de autorregulación se definen como:

a) La posibilidad que tienen los responsables y encargados de establecer y autoimponerse voluntariamente reglas para el debido tratamiento de datos personales que complementen lo previsto por la normativa, elevando los estándares de protección de ésta y considerando las particularidades de los responsables o encargados que desarrollan y adoptan esta clase de reglas
b) La posibilidad que tienen las personas titulares de los datos de establecer y autoimponerse voluntariamente reglas para el debido tratamiento de sus datos personales
c) La posibilidad que tienen las autoridades y el sector público de establecer reglas vinculantes para el debido tratamiento de datos personales que complementen lo previsto por la normativa, elevando los estándares de protección
d) La posibilidad que tienen los órganos garantes de la protección de datos personales de establecer reglas voluntarias para el debido tratamiento de datos personales que complementen lo previsto por la normativa, elevando los estándares de protección
e) Ninguna de las anteriores

10. ¿Cuál es la vigencia de la certificación de los esquemas de autorregulación?

a) Un año
b) Dos años
c) Cinco años
d) Diez años
e) No tienen vigencia