GUÍA DE AUDITORÍAS VOLUNTARIAS

EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

PARA EL SECTOR PÚBLICO

inai

DIRECTORIO

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Av. Insurgentes Sur 3211,
Col. Insurgentes Cuicuilco,
Alcaldía Coyoacán,
C.P. 04530, Ciudad de México.

Edición, agosto de 2023

ÍNDICE

5 **INTRODUCCIÓN**

7 **GLOSARIO**

13 **GENERALIDADES**

13 **¿Qué es una auditoría voluntaria?**

13 **¿Cuál es el objeto de una auditoría voluntaria?**

13 **¿Quién puede solicitar que se realice una auditoría voluntaria?**

13 **¿Ante quien se solicita una auditoría voluntaria?**

14 **¿Quiénes realizan las auditorías voluntarias?**

14 **¿Qué principios debe cumplir el equipo auditor?**

14 **¿Cuáles son las obligaciones del responsable auditado?**

14 **¿Se puede cancelar una auditoría voluntaria?**

14 **¿Cuánto dura el procedimiento de una auditoría voluntaria?**

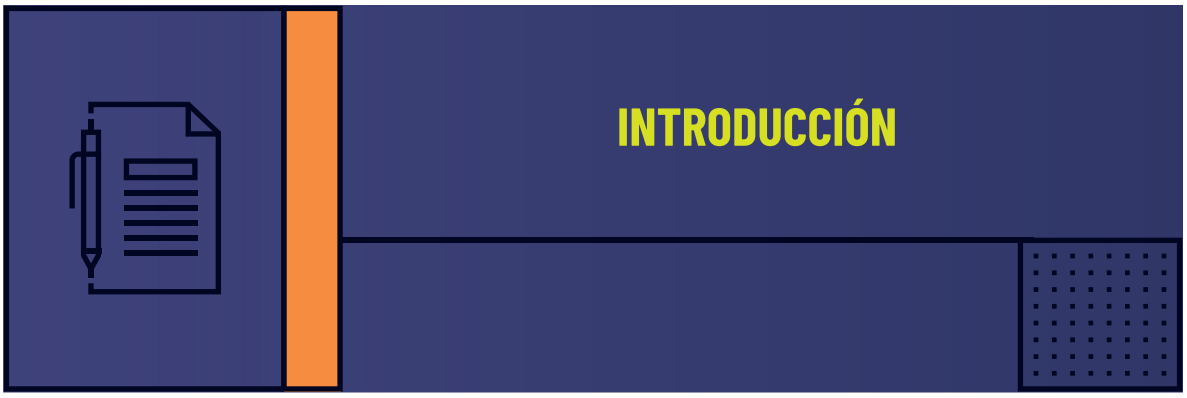
15 **¿Se aplica alguna sanción por las no conformidades determinadas en las auditorías?**

15 **Procedimiento de una auditoría voluntaria**

15 Solicitud de auditoría voluntaria

15 ¿Cuáles son los elementos que debe contener el escrito de solicitud de una auditoría voluntaria?

17 ¿Qué respuesta se da al escrito de solicitud de auditoría voluntaria?
17 Acuerdo de desechamiento
20 Acuerdo de inicio de la auditoría voluntaria
20 Acuerdo de requerimientos de información adicional
21 Revisión en auditorías voluntarias
21 Revisión documental
21 Revisión en sitio a través de visitas de auditoría
21 ¿Qué debe contener la orden de visita?
22 Listas de comprobación
22 ¿Qué revisa el INAI en una auditoría voluntaria dependiendo del alcance fijado?
23 ¿Qué revisa el equipo auditor en los Principios?
25 ¿Qué revisa el equipo auditor en otras Obligaciones?
27 ¿Qué revisa el equipo auditor en los Deberes?
29 Cédulas de conclusiones
29 Acuerdo de reunión de cierre de auditoría voluntaria
29 Reunión de cierre de auditoría voluntaria
30 ¿Qué contenido lleva el acta de cierre de auditoría?
30 Seguimiento de no conformidades de auditoría voluntaria
31 Cédulas de seguimiento
31 Acuerdo de finalización de expediente



INTRODUCCIÓN

La presente publicación está dirigida a los sujetos obligados del ámbito federal; a efecto de brindarles una herramienta para coadyuvar a tener mayor compresión sobre la naturaleza, los alcances, el procedimiento y cuáles son los beneficios de las auditorías voluntarias en materia de protección de datos personales que realiza el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en lo sucesivo INAI o Instituto).

Cabe destacar que el derecho humano a la protección de datos personales en nuestro país encuentra sustento en los artículos 6, Base A, fracción II y 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos[1]; por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante Ley General), como norma reglamentaria de los artículos citados, instituye en su artículo primero como objeto el de establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados, en el ámbito federal, estatal y municipal, así como cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, en los órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

En ese orden, en el artículo 151 de la Ley General, se establece que, los responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto o los Organismos Garantes Locales, según corresponda, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la Ley General y demás normativa que resulte aplicable.

Por otra parte, en los Lineamientos Generales de Protección de Datos Personales del Sector Público[2] (en lo sucesivo Lineamientos Generales), del artículo 218 al 231 se desarrollan las reglas que deberán regir el procedimiento de

1 Fecha de consulta 31 de mayo de 2023. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

2 Lineamientos Generales de Protección de Datos Personales para el Sector Publicados en el Diario Oficial de la Federación el 26 de enero de 2018, Fecha de consulta 31 de mayo de 2023. Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018#gsc.tab=0

auditorías voluntarias competencia de este Instituto previstas en la Ley General.

Para fijar el alcance de las auditorías se recurre a la Ley General, en los artículos 16 al 71 y del 83 al 87 sobre los cuales se estipula lo relativo a los principios, deberes y obligaciones que son susceptibles de criterios de auditorías voluntarias cuando el alcance de la misma es total, es decir sobre los citados principios, deberes y obligaciones; por su parte, los numerales 7 al 118 de los Lineamientos Generales, son los que regulan estos criterios de auditoría consistentes en analizar, según se defina el alcance de la auditoría voluntaria en lo referente a los principios, deberes y obligaciones en materia de protección de datos personales.

A su vez, el INAI, publicó el Manual de procedimientos para la realización de las auditorías voluntarias a que hace referencia el artículo 151 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[3] (en lo sucesivo Manual) en el cual, se establecen los requisitos, condiciones y el procedimiento para el desarrollo de las auditorías voluntarias a que hacen referencia los artículos 151 de la Ley General y 218 al 231 de los Lineamientos Generales.

Es por lo anterior, que de conformidad a las facultades del INAI se emite la presente Guía que, pretende proporcionar apoyo técnico a los sujetos obligados del ámbito federal, a efecto de facilitar la compresión de las auditorías voluntarias y contribuir con lo siguiente:

- Facilitar a los sujetos obligados la comprensión de las auditorías voluntarias tramitadas en el INAI.
- Proporcionar un material didáctico a los responsables en el sector público de tratamientos de datos personales, que les sirva de consulta y guía para la tramitación de una solicitud de auditoría voluntaria.
- Ofrecer a los responsables del tratamiento de datos personales del sector público un documento que les provea de una manera pormenorizada, pautas claras y sencillas del procedimiento de auditoría voluntaria.

3 Publicado en el DOF el 31 de agosto de 2018, Fecha de consulta 31 de mayo de 2023. Disponible en: https://www.dof.gob.mx/2018/INAI/ANEXO-ACT-PUB-08-08-2018.06.pdf

GLOSARIO[4]

Acción correctiva	Determinación emitida por el Instituto, que sugiere una acción en específico, que el responsable tiene la potestad de realizar para eliminar las causas de una no conformidad detectada.
Acción preventiva	Determinación emitida por el Instituto, que propone una acción en específico, que el responsable tiene la potestad de realizar para evitar que surja una situación no deseada que pudiera ocurrir y traer como consecuencia el incumplimiento a la Ley General y/o a los Lineamientos Generales.
Acta circunstanciada	Es el documento considerado como papel de trabajo en el cual se hacen constar hechos o circunstancias que el grupo auditor considere relevantes y necesarios para el cumplimiento de su función.
Acuerdo de visita	Documento por el cual se notifica al responsable la realización de la auditoría voluntaria en sitio por parte del grupo auditor, con el fin de asegurar el acceso y la recepción por parte del responsable auditado, de acuerdo con el alcance de la auditoría voluntaria.
Alcance de auditoría	Determinación de la extensión y los límites de la revisión que se realizará en la auditoría voluntaria, descripción de las áreas, tratamientos o procesos a auditar, y se determina incluir todos los principios, deberes y obligaciones a analizar en la auditoría, así como el periodo cubierto.

4 Con relación con el presente apartado, se hace la precisión que, algunos conceptos que aquí se definen, no se encuentran establecidos en la LGPDPPSO, los Lineamiento Generales ni en Manual de Auditorías Voluntarias, sin embargo, son utilizados en el procedimiento de auditoría voluntaria.

Áreas	Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan dar tratamiento, y ser personas responsables o encargadas de los datos personales.
Auditoría en sitio	Revisión en las instalaciones físicas del responsable de las políticas, programas, procedimientos, prácticas y acciones que fueron revisadas documentalmente, verificando que estas se llevan a cabo conforme a lo señalado, y de conformidad con los criterios de auditoría voluntaria.
Auditor Líder	Servidor público designado por el INAI, a través de la Secretaría de Protección de Datos Personales o la Dirección General de Prevención y Autorregulación para coordinar y dirigir las actividades que impliquen la auditoría voluntaria a realizar.
Bases de datos	Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización. [5]
Cédula de conclusiones	Documentos de trabajo en el que cada uno de los miembros del equipo auditor deberá hacer un registro del resultado de la auditoria voluntaria, tras considerar los objetivos de la auditoria y los hallazgos observados.
Cédula de seguimiento	Documento en el que se registran los avances, seguimiento e implementación que el responsable realice en los términos y plazos establecidos con base en las acciones correctivas, acciones preventivas y las recomendaciones determinadas en el informe de auditoría voluntaria.
Conclusiones de la auditoría	Es el resultado que se obtiene tras considerar los objetivos de la auditoría voluntaria y los hallazgos derivados de ésta.
Conformidad	La adecuación de los controles, mecanismos o procedimientos adoptados por el responsable para el cumplimiento de las obligaciones previstas en la Ley General, los Lineamientos Generales y cualquier otro criterio de auditoría.
Criterios de auditoría	Estarán conformados por lo dispuesto en la Ley General, los Lineamientos Generales, la normativa que resulte aplicable, así como las políticas, procedimientos o manuales que correspondan.

5 Diccionario de Protección de Datos Personales Conceptos Fundamentales. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Disponible en el siguiente enlace: https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

Cruces de auditoría	Es el enlace entre la información relacionada en las diferentes cédulas e informe de auditoría voluntaria; para aclaraciones con relación a un hallazgo específico; a fin de facilitar el trabajo de supervisión y conciliar los hallazgos identificados en la auditoría.
DAV	Dirección de Auditorías Voluntarias adscrita a la Dirección General de Prevención y Autorregulación.
DGEIVSP	Dirección General de Evaluación, Investigación y Verificación del Sector Público, adscrita a la Secretaría de Protección de Datos Personales del INAI.
DGPAR	Dirección General de Prevención y Autorregulación, adscrita a la Secretaría de Protección de Datos Personales del INAI, área facultada para la atención y tramitación de solicitudes de auditorías voluntarias en materia de protección de datos personales.
Datos personales	Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
Datos personales sensibles	Aquellos que se refieren a la esfera más íntima de la persona titular, o cuya utilización indebida puede dar origen a discriminación que conlleve un riesgo grave para este. De manera enunciativa más no limitativa, se consideran sensibles lo datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.
Encargado	La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.
Evidencia de auditoría voluntaria	Es toda aquella información verificable que presente el responsable o de la que se allegue el Instituto por otros medios. Que sea pertinente para demostrar la conformidad con los criterios de la auditoría voluntaria a la cual se está sometiendo. Pueden ser registros, declaraciones de hechos, o cualquier otro tipo de información que sea oportuna para el análisis llevado a cabo en la auditoría voluntaria.

Experto técnico	Persona que emite opinión técnica al equipo auditor, sobre diversos temas que se le consulta. que puede o no estar adscrito al INAI. En caso de requerirse la contratación de un experto técnico para la sustanciación de la auditoria voluntaria, correrá a cargo del responsable y dependerá de la disponibilidad presupuestal y los criterios de ejercicio de recursos públicos y austeridad que se encuentren vigentes. Los especialistas técnicos externos estarán obligados a guardar reserva o confidencialidad de la información a la que tengan acceso en virtud de su participación en la auditoria, y los informes que emitan estarán sujetos a lo dispuesto por las leyes de transparencia en lo que resulte conducente.
Grupo auditor	Personas servidoras públicas designadas en el acuerdo de inicio de auditoría por la DGPAR, que llevan a cabo los trabajos de la auditoría voluntaria, con el apoyo, si es necesario, de expertos técnicos adscritos al INAI o aquellos que, sean contratados para tal efecto.
Hallazgos de auditoría	Resultados de la valoración y revisión de la evidencia recopilada en la auditoría voluntaria, en contraste con el objetivo, alcance y los criterios establecidos.
Informe final de auditoría	Es el documento que señala los resultados obtenidos de la auditoría voluntaria y se pronuncia sobre la conformidad o no conformidad de los controles, mecanismos o procedimientos adoptados por el responsable auditado para el cumplimiento de las obligaciones previstas en la Ley General, los Lineamientos Generales, la normativa que haya sido señalada como criterio de auditoría, así como las políticas, procedimientos o manuales que correspondan, respecto del tratamiento de datos personales auditado, y en función del alcance de la auditoría voluntaria. En el que se deberá orientar al responsable sobre el fortalecimiento y un mejor cumplimiento de las obligaciones previstas en la normatividad, señalando medidas, acciones, recomendaciones y sugerencias específicas, de carácter preventivo y/o correctivo, en función de las características generales y particularidades del tratamiento de datos personales y de los hallazgos obtenidos en la auditoría.
Lista de verificación	Documento que muestra el análisis de la información, con base en el desarrollo de los procedimientos realizados durante la auditoría voluntaria.

Nota de auditor	Comentarios que el auditor considera necesarios para definir los diferentes rubros en el desarrollo de la auditoría voluntaria, que le permitirán direccionar las etapas de planeación y ejecución hacia procesos críticos y relevantes, para emitir un informe e incorporarlo a la clasificación del contenido de la cédula.
No conformidad	Es la inadecuación de los controles, mecanismos o procedimientos adoptados por el responsable auditado respecto de las obligaciones previstas en la Ley General, Lineamientos Generales y cualquier otro criterio de auditoría voluntaria.
Plan de visita	Es la descripción de cada una de las actividades y detalles acordados para efectuar la visita de auditoría por parte del equipo auditor en las instalaciones del sujeto obligado, el cual puede ser modificado en cualquier momento previo acuerdo entre las partes.
Políticas y programas de protección de datos personales	Con base al cumplimiento del artículo 30, fracciones I y II de la Ley General y artículo 47 de los Lineamientos Generales, el responsable deberá elaborar e implementar políticas y programas de protección de datos personales con el objeto de establecer los elementos y actividades de dirección, operación y control de todos sus procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continua- obligatorios y exigibles al interior de la organización del responsable.
Principios en materia de protección de datos personales	Los sujetos obligados, en el tratamiento de datos personales, deberán observar los principios de calidad, consentimiento, finalidad, información, lealtad, licitud, proporcionalidad y responsabilidad.
Programa anual de auditorías voluntarias	La DGPAR en conjunto con la Secretaría de Protección de Datos Personales, elaborará un programa anual de auditorías voluntarias, en el cual se señalarán los elementos que justifican la selección de sujetos obligados responsables propuestos para remitir una invitación, con la finalidad de exhortarlos a solicitar una auditoría voluntaria en materia de protección de datos personales ante el Instituto.
Recomendaciones	Es un planteamiento objetivo, normativo, aplicable y específico para la atención de las no conformidades determinadas en la auditoría voluntaria.

Responsable solicitante	Es el sujeto obligado de la LGPDPPSO, del ámbito federal, responsable del tratamiento de los datos personales y quien solicita la auditoría.
SGSPD	Sistema de Gestión de Seguridad de Datos Personales.
SPDP	Secretaría de Protección de Datos Personales del INAI.
Persona titular	La persona física a quien corresponden los datos personales.
Tratamiento	Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

GENERALIDADES

¿Qué es una auditoría voluntaria?

Es un proceso sistemático, independiente y documentado, iniciado por solicitud de un responsable al Instituto, enfocado a evaluar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados por los responsables para el tratamiento de datos personales, para la obtención de evidencia que permita determinar su conformidad con las disposiciones previstas en la Ley General, los Lineamientos Generales y demás normativa aplicable.

¿Cuál es el objeto de una auditoría voluntaria?

Las auditorías voluntarias tienen la finalidad primordial de efectuar una evaluación de la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados por un sujeto obligado para el cumplimiento de las disposiciones previstas en la Ley General, los Lineamientos Generales y la normativa que resulte aplicable.

Además, se debe tener presente que las auditorías voluntarias son de carácter preventivo y no punitivo, por lo que, a partir del resultado de una auditoría voluntaria, la DGPAR no podrá realizar acciones para que dé inicio un procedimiento de verificación o sancionatorio.

¿Quién puede solicitar que se realice una auditoría voluntaria?

El Instituto puede enviar una invitación a sujetos obligados para exhortarlos a que soliciten una auditoría voluntaria (misma que se deriva del Programa Anual de Auditorías Voluntarias); sin embargo, los responsables del ámbito federal pueden solicitar someterse a una auditoría voluntaria ante el Instituto, independientemente de que hayan recibido o no la invitación por parte del INAI.

¿Ante quien se solicita una auditoría voluntaria?

El responsable solicitante deberá presentar directamente su solicitud en el domicilio del Instituto[6] o bien a través de del correo electrónico auditoriasvoluntarias@inai.org.mx, en el formato establecido para ello.

6 Domicilio del INAI: Insurgentes Sur 3211, Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán, Ciudad de México, C.P. 04530.

¿Quiénes realizan las auditorías voluntarias?

Un equipo auditor estará conformado por las personas servidoras públicas adscritas a la DGPAR, así como por aquellos expertos técnicos que, en su caso, podrán apoyar al personal de dicha unidad administrativa en el desarrollo de las auditorías.

¿Qué principios debe cumplir el equipo auditor?

En la práctica de sus funciones, el auditor se apegará a los principios éticos de legalidad, honradez, lealtad, imparcialidad, eficiencia, disciplina, profesionalismo, objetividad, transparencia, redición de cuentas, eficacia, integridad, reserva y confidencialidad, establecidos en el Estatuto Orgánico y en el Código de Ética del Instituto.

El auditor deberá adoptar una actitud de independencia de criterio respecto del responsable, y se mantendrá libre de cualquier situación que pudiera señalarse como incompatible con su objetividad.

Se encontrará impedido de recibir cualquier tipo de atención o beneficio ya sea económico o en especie, para sí o para otro, provenientes de personas físicas o jurídicas vinculadas al responsable, o al procedimiento de auditoría voluntaria.

¿Cuáles son las obligaciones del responsable auditado?

- Proporcionar y mantener a disposición de los auditores autorizados por el Instituto, la información, documentación o datos relacionados con el tratamiento de datos personales objeto de la auditoría voluntaria;
- Permitir y facilitar a los auditores autorizados del Instituto el acceso a archiveros, registros, archivos, sistemas, equipos de cómputo, discos o cualquier otro medio o sistema de tratamiento de los datos personales objeto de la auditoria voluntaria;
- Permitir el acceso a los auditores autorizados por el Instituto al lugar, a las oficinas o instalaciones del responsable donde se lleve a cabo el tratamiento de datos personales auditado, y
- El responsable auditado no podrá negar el acceso a la información y documentación relacionada con el tratamiento de datos personales auditado, ni podrá invocar la reserva o la confidencialidad de la información en términos de lo dispuesto en la normatividad que resulte aplicable.

¿Se puede cancelar una auditoría voluntaria?

El responsable o la DGPAR podrán cancelar la auditoría voluntaria en cualquier fase de su ejecución, cuando existan razones que lo justifiquen, siempre y cuando se realice la notificación formal de ello a la otra parte.

¿Cuánto dura el procedimiento de una auditoría voluntaria?

El INAI deberá realizar la auditoría voluntaria en un plazo de cincuenta días,

contados a partir del día siguiente de la fecha que se haya señalado en el acuerdo de inicio. Este plazo podrá ampliarse por un periodo igual, y por una sola vez, cuando existan razones que lo justifiquen, teniendo en cuenta las circunstancias específicas del caso, supuesto que deberá siempre de notificarse al solicitante.

¿Se aplica alguna sanción por las no conformidades determinadas en las auditorías?

Las auditorías voluntarias son de carácter preventivo y no punitivo, por lo que, a partir del resultado de una auditoría voluntaria, el INAI no podrá realizar acciones para que dé inicio un procedimiento de verificación o sancionatorio.

Procedimiento de una auditoría voluntaria

Durante el procedimiento de una auditoría voluntaria, deberá constar el proceso de esta, desde su preparación e inicio, desarrollo, conclusión y cierre, hasta el seguimiento de no conformidades de auditoría voluntaria, en su caso; por lo cual, se tendrán que emitir las siguientes actuaciones que deben obrar en el expediente de la auditoría voluntaria.

¿Cuáles son las fases del proceso de una auditoría?

I. **Preparación e inicio de la auditoría voluntaria.**
II. **Desarrollo.**
III. **Conclusión y cierre de la auditoría voluntaria.**
IV. **Seguimiento de no conformidades de auditoría voluntaria.**

I. Preparación e inicio de la auditoría voluntaria

Solicitud de auditoría voluntaria

Es el escrito presentado por el sujeto obligado del ámbito federal ante el INAI, a través del cual solicita someterse a una auditoría voluntaria en materia de protección de datos personales.

¿Cuáles son los elementos que debe contener el escrito de solicitud de una auditoría voluntaria?

El sujeto obligado debe revisar que su escrito de solicitud de auditoría voluntaria contenga los siguientes elementos, que son los necesarios para la admisión de una auditoría voluntaria ante el INAI.

Consecutivo	Elemento	Cuento con el dato
1	La denominación y el domicilio del responsable solicitante	
2	Las personas autorizadas para oír y recibir notificaciones	

<table>
<tr><th>Consecutivo</th><th>Elemento</th><th>Cuento con el dato</th></tr>
<tr><td>3</td><td>La descripción del tratamiento de datos personales que se pretende someter a la auditoría voluntaria, indicando, de manera enunciativa más no limitativa:
<table>
<tr><th>Elementos en la descripción del tratamiento</th><th>Cuento con el dato</th></tr>
<tr><td>Las finalidades de éste.</td><td></td></tr>
<tr><td>El tipo de datos personales tratados.</td><td></td></tr>
<tr><td>Las categorías de personas titulares involucradas.</td><td></td></tr>
<tr><td>Las transferencias que, en su caso, se realicen.</td><td></td></tr>
<tr><td>Las medidas de seguridad implementadas.</td><td></td></tr>
<tr><td>La tecnología utilizada, así como cualquier otra información relevante del tratamiento a auditar.</td><td></td></tr>
</table></td><td></td></tr>
<tr><td>4</td><td>Las circunstancias o razones que lo motivan a someterse a una auditoría voluntaria.</td><td></td></tr>
<tr><td>5</td><td>El nombre, cargo y firma de quien solicite la auditoría voluntaria.

Podrá ser:
La persona titular de la dependencia o entidad u homólogo.
La persona titular de la unidad administrativa u homólogo que será auditada.
El Oficial de Protección de Datos Personales del responsable o la persona Presidente del Comité de Transparencia.</td><td></td></tr>
<tr><td>6</td><td>Cualquier otra información o documentación que considere relevante hacer del conocimiento del Instituto.</td><td></td></tr>
<tr><td>7</td><td>El responsable solicitante deberá especificar denominación y domicilio del área que está a cargo del tratamiento a auditar.</td><td></td></tr>
</table>

Una vez que se ingresa el escrito de solicitud de auditoría voluntaria, la DGPAR procede a:

- **Emitir el oficio de solicitud de información a la DGEIVSP**

  En el término de tres días hábiles posteriores a la recepción de la solicitud, la DGPAR envía un oficio a la DGEIVSP, a efecto de que informe si existe algún procedimiento de verificación, denuncia, o verificación de oficio programada al sujeto obligado con el objeto de determinar la procedencia de la solicitud de auditoría voluntaria.

- **Respuesta de la DGEIVSP**

  La DGEIVSP informa a la DGPAR si existe o no algún procedimiento de verificación, denuncia, o verificación de oficio programada al sujeto obligado con el objeto de determinar la procedencia de la solicitud.

¿Qué respuesta se da al escrito de solicitud de auditoría voluntaria?

Acuerdo de desechamiento

La solicitud de la auditoría voluntaria será desechada por improcedente cuando:

1. El Instituto tenga conocimiento de una denuncia en materia de protección de datos personales en contra del responsable solicitante, o bien, se esté sustanciando un procedimiento de verificación relacionado con el mismo o similar tratamiento de datos personales que se pretende someter a la auditoría voluntaria.

Ejemplo: Cuando la DGEIVSP tras responder el requerimiento realizado por la DGPAR, informa a ésta última que existe algún procedimiento de verificación, denuncia, o verificación de oficio programada al sujeto obligado.

2. El responsable se encuentre seleccionado de oficio para ser verificado por parte del Instituto.

Ejemplo: Cuando la DGEIVSP tras responder el requerimiento realizado por la DGPAR, informa a ésta última que la parte responsable se encuentra seleccionada de oficio para ser verificada por parte del Instituto.

3. El Instituto no sea competente.

Ejemplo: Cuando un sujeto obligado del ámbito municipal, ingresa una solicitud de auditoría voluntaria ante el INAI, no es procedente su admisión, debido a que el INAI únicamente puede auditar a sujetos obligados del ámbito federal.

4. Se encuentre en trámite una solicitud idéntica por parte del mismo responsable.

Ejemplo: Un sujeto obligado denominado “X” solicita una auditoría voluntaria en el sistema de gestión o tratamiento de datos “Y” de la unidad administrativa “A”; y en el INAI, ya se esta llevando a cabo una auditoría con el mismo sujeto obligado, sobre el mismo tratamiento de datos y de la misma unidad administrativa.

5. El área a auditar no forma parte del responsable solicitante.

Ejemplo: El sujeto obligado llamado “B” solicita una auditoría voluntaria

en materia de protección de datos personales sobre el tratamiento de datos "Y" de la unidad administrativa "A" que se encuentra adscrita a otro sujeto obligado denominado "C"; por lo que como bien puede observarse el sujeto obligado solicitante de la auditoría voluntaria es diverso al sujeto obligado al que se encuentra adscrita la unidad administrativa que realiza el tratamiento y al cual se solicita auditar, por tanto, es una causal de desechamiento de la solicitud de auditoría voluntaria.

6. No se trate de una solicitud de auditoría voluntaria en materia de protección de datos personales.

Ejemplo: Cuando el sujeto obligado "W" solicita una auditoría voluntaria en materia de Obligaciones de Transparencia. Es improcedente debido a que las auditorías voluntarias motivo de la presente Guía, son únicamente en materia de protección de datos personales, por tanto, dicha solicitud tendría que desecharse

7. El sujeto obligado no responda en el término legal concedido al acuerdo de prevención que, en su caso, le realice el INAI.

Ejemplo: El sujeto obligado denominado "L" solicita una auditoría voluntaria en materia de protección de datos personales, sin embargo, en su escrito de solicitud no asienta el nombre, cargo y firma del servidor público que presenta la auditoría voluntaria, por lo cual, la DGPAR notifica un acuerdo para que en el término legal máximo de 10 días subsane la omisión, sin embargo, una vez transcurrido el término legal otorgado en el requerimiento, no se recibió respuesta del sujeto obligado.

La consecuencia a dicha omisión será el no tener por presentada la solicitud de auditoría voluntaria y desecharla.

Acuerdo de prevención

El INAI podrá requerir información al responsable solicitante, en caso de que la solicitud no sea clara, o bien, se omita manifestar uno o más de los requisitos necesarios y no se cuente con elementos para subsanarlos.

A partir de la notificación del requerimiento de información, se suspenderá el plazo que tiene el Instituto para emitir su respuesta a la solicitud, por lo que se reanudará el cómputo de dicho plazo a partir del día siguiente de su desahogo.

El responsable tendrá un plazo máximo de diez días, contados a partir del día siguiente de la notificación del requerimiento de información, para que subsane las omisiones de su solicitud.

Acuerdo de admisión

El INAI emite el acuerdo de admisión siempre y cuando se actualicen los siguientes supuestos:

- El sujeto obligado cumpla con los requisitos en su escrito de solicitud de auditoría voluntaria.
- La DGEIVSP, informe a la DGPAR que no existe algún procedimiento de verificación, denuncia, o verificación de oficio programada al sujeto con obligado que solicita la auditoría voluntaria.
- El sujeto obligado atienda de manera satisfactoria al acuerdo de prevención, en su caso.

En el supuesto de que el responsable solicite que sea auditado más de un tratamiento o área, la DGPAR determinará la procedencia de auditar todos los tratamientos o áreas en una misma auditoría, o si es pertinente atenderlos en diversas auditorías. La determinación al respecto será informada al responsable solicitante.

La DGPAR deberá notificar al responsable el acuerdo de admisión o de no presentación, dentro de los tres días siguientes contados a partir del día de su emisión.

Reunión preparatoria

El INAI y el sujeto obligado fijan fecha para llevar a cabo una reunión preparatoria; y una vez acordada entre las partes, la DGPAR emite un acuerdo para formalizar la fecha estipulada y se notifica al sujeto obligado.

La reunión preparatoria tiene por objeto:

- Que el grupo auditor conozca los antecedentes y generalidades del tratamiento de datos personales que serán sometidos a la auditoría voluntaria.
- Que se consideren los objetivos de la auditoría voluntaria.
- Que se identifique con precisión el alcance de la auditoría voluntaria.
- Conocer la información o documentación que sea requerida por la DGPAR para continuar con el procedimiento.
- Acordar la fecha de inicio de la auditoría voluntaria.

Una vez concluida la reunión preparatoria el equipo auditor emite un acta circunstanciada que deberá ser firmada por los asistentes, en la cual se asienta lo siguiente:

- El lugar, fecha y hora de realización de la visita, diligencia y/o reunión de trabajo.
- La denominación del responsable;
- El nombre completo y cargo de la persona servidora pública que atendió la reunión de trabajo.
- Los nombres completos y cargos de todas las personas servidoras públicas que intervinieron.
- La narración circunstanciada de los hechos ocurridos durante la reunión de trabajo.
- El nombre completo y firma de la persona servidora pública que representa al Instituto, así como al responsable.

Al fijar el alcance de la auditoría voluntaria, se deberá establecer los principios, deberes y obligaciones de la Ley General que serán evaluados en el desarrollo de la auditoría voluntaria.

Ahora bien, en el siguiente párrafo se da un ejemplo de cómo se delimita el alcance parcial de una auditoría voluntaria:

El alcance de la auditoría voluntaria que se realizará será respecto del tratamiento de datos personales denominado "Solicitudes de Derechos ARCO" en la Unidad de Transparencia del sujeto obligado "F", para el cumplimiento de las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y Lineamientos Generales de Protección de Datos Personales para el Sector Público, con el objeto

de evaluar su adaptación, adecuación y eficacia de los principios de licitud, lealtad, información, consentimiento, finalidad, responsabilidad, calidad y proporcionalidad, previstos en la Ley General, implementados al 01 diciembre 2023.

Y si queremos ejemplificar un alcance total en el cual se analicen los principios, deberes y obligaciones sería de la siguiente forma:

El alcance de la auditoría voluntaria que se realizará será respecto del tratamiento de datos personales denominado "Auditorías Voluntarias" en la Dirección "G" del sujeto obligado "K", para el cumplimiento de las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y Lineamientos Generales de Protección de Datos Personales para el Sector Público, con el objeto de evaluar su adaptación, adecuación y eficacia de los principios, deberes y obligaciones, previstos en la Ley General, implementados al 01 diciembre 2023.

II. Desarrollo de auditoría voluntaria

Acuerdo de inicio de la auditoría voluntaria

La DGPAR emitirá un acuerdo de inicio, el cual deberá contener, entre otros, los siguientes elementos:

- Fecha de inicio de la auditoría voluntaria.
- La persona servidora pública que fungirá como auditor líder, quien será encargada de la coordinación de la auditoría voluntaria.
- Los objetivos de la auditoría voluntaria.
- El alcance de la auditoría voluntaria, incluyendo la identificación del área a auditar; el tratamiento de datos personales; las finalidades del tratamiento; el tipo de datos personales tratados; las categorías de titulares involucrados; las transferencias que, en su caso, se realicen; las medidas de seguridad implementadas; la tecnología utilizada, entre otros elementos.
- Los criterios de auditoría.
- La persona servidora pública facultada para representar al responsable solicitante en la auditoría voluntaria.
- Los asuntos relacionados con la confidencialidad y la seguridad de la información.
- Requerimientos de información y documentación relacionada con el tratamiento de datos personales que se someterá a la auditoría voluntaria, adicional a la que se haya aportado en la solicitud y en la reunión de trabajo, que resulte necesaria para continuar con el desarrollo de la auditoría.

Acuerdo de requerimiento de información adicional

La DGPAR podrá requerir al responsable documentación e información que esté vinculada con el tratamiento objeto de la auditoría, en cualquier momento de su preparación, desarrollo o fase de conclusión.

El requerimiento deberá estar fundado y motivado, describir de manera clara y

precisa la información y documentación solicitada y señalar el plazo y, en su caso, los términos para responderlo.

En caso de que existan circunstancias que impidan al responsable solicitante responder el requerimiento en el plazo señalado por la DGPAR, esta última podrá ampliar el plazo, previa solicitud por escrito del responsable.

Revisión en auditorías voluntarias

Las auditorías voluntarias solicitadas ante el Instituto podrán ser desahogadas a través de revisión documental y/o revisión en sitio por medio de visitas de auditoría.

Revisión documental

El INAI requiere al responsable solicitante la documentación e información necesaria vinculada con el tratamiento de datos personales auditado, a fin de revisarla en sus oficinas para determinar si las políticas, programas, procedimientos, prácticas o cualquier otra acción documentada es acorde a la Ley General, los Lineamientos Generales y demás normatividad aplicable.

Revisión en sitio a través de visitas de auditoría

En caso de ser necesaria una revisión en sitio, el INAI emite un acuerdo y el equipo auditor acude a las oficinas o instalaciones donde se lleva cabo el tratamiento de datos personales auditado, para revisar que en los hechos se esté operando como se señala en la documentación analizada en la revisión documental y de conformidad con los criterios de auditoría del tratamiento de datos personales materia de la auditoría.

¿Qué debe contener la orden de visita?

- La fecha en que se emite la orden.
- La denominación del responsable solicitante y su domicilio.
- El nombre y cargo del personal designado por la DGPAR para la realización de la visita de auditoría;
- La descripción clara y precisa de los objetivos y alcances de la visita de auditoría, los cuales deberán estar relacionados con el tratamiento de datos personales que está siendo auditado.
- La solicitud al responsable solicitante para que designe a los servidores públicos o personas que atenderán la visita de auditoría voluntaria.
- La fecha y hora en que se realizará la visita de auditoría voluntaria.
- La firma autógrafa de la persona servidora pública que expide la orden de visita.
- La denominación de la unidad administrativa y los domicilios en los que se realizará la visita de auditoría voluntaria.
- Los recursos e instalaciones que necesita el equipo auditor que estén disponibles para el desarrollo de la visita de auditoria voluntaria.
- La solicitud al responsable solicitante para que informe, en su caso, sobre la clasificación de información como reservada o confidencial, así como las medidas de seguridad que se requieran considerar para la visita.
- Cualquier otra información o requerimiento que determine necesario la DGPAR, según las circunstancias particulares de la auditarla voluntaria.

Siempre que se realice una revisión en sitio a través de visitas de auditoría, deberá suscribirse un acta de la revisión en sitio.

Listas de comprobación

Las listas de comprobación forman parte de los papeles de trabajo y documentación soporte del equipo auditor, en las mismas se plasman y desarrollan los rubros siguientes:

Contenido
Nombre del responsable que solicitó la auditoría voluntaria
Nombre del área específica por auditar
Proceso o tratamiento de datos personales por auditar
Nombre de las personas integrantes del equipo auditor que realiza la auditoría voluntaria
Ley, lineamiento o normatividad a revisar (criterio de auditoría)
Artículo, o disposición específica a revisar
Número de expediente de auditoría voluntaria
Fecha en que se realiza la evaluación
Hora de inicio
Hora de conclusión
Principio, deber u obligación a revisar
Descripción del Principio, deber u obligación a revisar
Describir la comprobación de la adecuación
Describir la evidencia presentada por el responsable
Nombre y cargo de la persona que funge como auditor líder
Nombre y cargo de la persona auditora quien realiza la revisión

¿Qué revisa el INAI en una auditoría voluntaria dependiendo del alcance fijado?

En este apartado vamos a citar documentos y/o evidencia que, dependiendo del alcance señalado en la auditoría voluntaria, es decir, si se fijaron los principios, deberes u obligaciones; pudieran presentar los sujetos obligados a efecto de que el equipo auditor se encuentre en posibilidad de verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la LGPDPPSO, Lineamientos Generales y demás normativa aplicable.

En relación con el párrafo anterior, se hace hincapié en dos puntos importantes:

- El equipo auditor realiza el análisis de los documentos y evidencia presentados por el sujeto obligado y/o recabados por otros medios; y comprueba que se observen las dispocisiones establecidas en la Ley General, Lineamientos Generales y demás normativa aplicable.
- Los documentos que se indicarán en párrafos subsecuentes, son de forma enunciativa, más no limitativa, con la única finalidad de orientar a las personas servidoras públicas responsables del tratamiento de los datos personales, para que las mismas cuenten con ejemplos para el caso de que pretendan someterse a una auditoría voluntaria, sin que ello implique que únicamente con tales documentales se cumpla con lo establecido por la Ley General, los Lineamientos Generales y demás normativa aplicable.

¿Qué revisa el equipo auditor en los Principios?

Principio de Licitud
La normatividad que señale el SO respecto al tratamiento de datos personales en los siguientes documentos: • Aviso de privacidad integral y simplificado correspondiente al tratamiento que se esté auditando. • Documento de seguridad. • Programa de protección de datos personales.

Principio de Finalidad
Aviso de privacidad integral y simplificado correspondiente al tratamiento que se vaya a auditar.
Documental que justifique que el tratamiento de los datos personales cuenta con finalidades concretas, lícitas, explícitas y legítimas.
Las finalidades deben estar relacionadas con las atribuciones normativas de la unidad administrativa que realice el tratamiento.

Principio de Lealtad
Aviso de privacidad integral y simplificado correspondiente al tratamiento que se vaya a auditar.
Resultados de las auditorías o procedimientos de revisión efectuados.

Principio de Consentimiento
Aviso de privacidad integral y simplificado correspondiente al tratamiento que se vaya a auditar.
Procedimiento o medio por el que se pone a disposición de las personas titulares el aviso de privacidad del tratamiento que se vaya a auditar.
Documento en el que conste que las solicitudes de consentimiento estén redactadas de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas e inteligibles, se encuentren redactadas en un lenguaje claro y sencillo acorde con el perfil de la persona titular, y se distingan de asuntos ajenos a la protección de datos personales (p.e. el aviso de privacidad).
Consentimiento expreso otorgado por los titulares y la solicitud respectiva, en su caso.
Documento en el que se encuentren identificadas las finalidades para las cuales se requiere el consentimiento.

Documento con el que se acredite que cuando los datos personales se recaben directamente del titular, y se requiera el consentimiento, éste deberá solicitarse previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad.
Documento con el que se acredite que cuando los datos personales se obtengan indirectamente del titular, y se requiera el consentimiento, no se podrán tratar los datos personales hasta que se cuente con la manifestación libre, específica e informada del titular, en la que autorice el tratamiento de sus datos personales de manera tácita o expresa, según corresponda.
Documental que demuestre que se cuenta con un mecanismo para atender las solicitudes de revocación del consentimiento, mismas que podrán ser presentadas por el titular en cualquier momento del tratamiento sin que se le atribuyan efectos retroactivos, a través del ejercicio de los derechos de oposición y cancelación.
Documental que acredite que se atienden las reglas de representación previstas en el Código Civil Federal y demás disposiciones que resulten aplicables en la materia específica de que se trate, para la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, en su caso.
Principio de Calidad
Documento que contenga el procedimiento o mecanismo para la conservación, bloqueo previo a la supresión; y supresión de los datos personales en el tratamiento que se vaya a auditar, así como la evidencia de su implementación.
Documento en el que conste el mecanismo a través del cual se mantienen exactos, completos y actualizados los datos personales (p.e. procedimientos, programas, lineamientos o políticas, así como la evidencia de su implementación en el tratamiento auditado).
Principio de Proporcionalidad
Documentos en los que se acredite que el tratamiento de los datos personales resulta **adecuado, relevante** y **estrictamente necesario** para la finalidad que justifica su tratamiento. Se tienen **identificados los datos personales** que se requieren para cada una de las finalidades. Los datos personales que se solicitan son los **mínimos** necesarios para cumplir con las finalidades. • Aviso de privacidad integral y simplificado correspondiente al tratamiento que se vaya a auditar. • Documentos, expedientes, archivos correspondientes al tratamiento. • Normatividad. • Inventario de DP

Principio de Información
Aviso de privacidad integral y simplificado correspondiente al tratamiento que se vaya a auditar.
Procedimiento o medio por el que se pone a disposición de la persona titular el aviso de privacidad del tratamiento que se vaya a auditar.
Documento en el que conste que las solicitudes de consentimiento estén redactadas de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas e inteligibles, formuladas en un lenguaje claro y sencillo acorde con el perfil del titular, y se distingan de asuntos ajenos a la protección de datos personales (p.e. el aviso de privacidad).
Documento que contenga el procedimiento o mecanismo a través del cual se obtiene el consentimiento expreso.

Principio de Responsabilidad
Documento con el cual acredite que destina recursos autorizados para la instrumentación de programas y políticas de protección de datos personales.
Programa de protección de datos personales, aprobado, coordinado y supervisado por el Comité de Transparencia del sujeto obligado de que se trate, obligatorio y exigible al interior de su organización. Políticas de protección de datos personales, obligatorias y exigibles al interior de su organización.
Programa de capacitación y actualización de las personas servidoras públicas sobre las obligaciones y deberes en materia de protección de datos personales y evidencia con la cual se acredite que se puso en práctica dicho programa.
Documento que contenga los mecanismos de supervisión y vigilancia interna y/o externa, incluyendo auditorías para comprobar el cumplimiento de las políticas de protección de datos personales, así como la evidencia de su implementación en el tratamiento auditado.
Documento que contenga el procedimiento para recibir y responder dudas y quejas de los titulares, así como la evidencia de su implementación en el tratamiento auditado.
Documento que acredite que para el desarrollo del sistema en el que se tratan los datos personales que se auditará, en su caso, se diseñó, desarrolló e implementó tomando en cuenta la privacidad por diseño.

¿Qué revisa el equipo auditor en otras Obligaciones?

Derechos ARCO
Procedimiento para atención de solicitudes de derechos ARCO.
Medios disponibles para la presentación de solicitudes de ejercicio de derechos ARCO.
Formatos y guías.

Acuerdos adoptados con **instituciones públicas especializadas.**
Respuesta y documentación que acredite el ejercicio del derecho por parte de la persona titular. (p.e. notificación de la ampliación del plazo de respuesta).
Documentación generada para acreditar la identidad de la persona titular y, en su caso, la identidad y personalidad de su representante.

Comité de Transparencia
Se cuenta con un Comité de Transparencia. (p.e. un acta de sesión del Comité de Transparencia o algún documento que acredite el nombramiento de los integrantes).
Programa de trabajo para la implementación del Programa de Protección de Datos Personales, así como la evidencia de su implementación en el tratamiento auditado.
Procedimiento o mecanismo para supervisar el cumplimiento del documento de seguridad, así como la evidencia de su implementación en el tratamiento auditado.
Programa de capacitación y actualización para los servidores públicos, en materia de protección de datos personales, así como la evidencia de su implementación en el tratamiento auditado.

Unidad de Transparencia
Se cuenta con una Unidad de Transparencia.
Procedimientos internos para realizar las funciones y gestionar de manera eficiente las **solicitudes de derechos ARCO** y auxiliar y orientar a los titulares en la presentación de las solicitudes.
Metodología para la aplicación de **evaluaciones de calidad** sobre la gestión de las solicitudes de ejercicio de derechos ARCO.

Portabilidad
Documentación que se genere para atender las solicitudes de ejercicio del derecho de portabilidad, (tomando en consideración el ACUERDO mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales).

Relación del Responsable y Encargado y Cómputo en la nube
Contrato marco con encargados, en el caso de que se tengan encargados
Cláusulas contractuales. (p.e. cláusulas tipo en contrato o instrumento jurídico a través de la cual se contratan servicios de cómputo en la nube).
Convenios de colaboración u otros instrumentos jurídicos.
Evidencia de la comunicación del aviso de privacidad.
Consentimiento de los titulares.

Transferencias
Cláusulas contractuales.
Convenios de colaboración u otros instrumentos jurídicos.
Evidencia de la comunicación del aviso de privacidad. (**Comunicar el aviso de privacidad respectivo** al tercero receptor en las transferencias nacionales e internacionales que se realicen).
Consentimiento de los titulares. (Solicitar el **consentimiento para las transferencias nacionales e internacionales**, en su caso).
Documento en el que se establezca el procedimiento en que se comunica el aviso de privacidad a los receptores de los datos personales.

¿Qué revisa el equipo auditor en los Deberes?

Deber de Confidencialidad
Controles definidos para la confidencialidad de los datos personales.
Documentación que acredite la implementación de los controles definidos (p.e convenios, contratos, responsivas entre otros).
Contrato marco con encargados, en el caso de que se tengan encargados.

Deber de seguridad
Documento de seguridad, así como la evidencia de su implementación en el tratamiento auditado. • Inventario de Datos Personales y de los Sistemas de Tratamiento • Funciones y obligaciones de las personas servidoras públicas que tratan datos personales • Análisis de riesgos • Análisis de brecha • Plan de trabajo • Mecanismos de Monitoreo y Revisión de las medidas de seguridad • Programa general de capacitación
Código de conducta.
Mecanismos que se emplean para dar a conocer las funciones y obligaciones del personal que trata los datos personales, así como la evidencia de su implementación en el tratamiento auditado.

Formatos físicos y electrónicos (capturas de pantallas) del sistema que se auditará, esquemas, diagramas, bocetos o cualquier elemento grafico que enliste los elementos informáticos (servidores, routers, dispositivos, etc.) y de los sistemas de tratamiento con los cuáles interactúa y hacen operar el sistema a revisar.
Catálogo de formatos de almacenamiento donde se especifique la ubicación física o electrónica de los datos personales.
Plan de continuidad del negocio y plan de recuperación de desastres modelos de carta de confidencialidad, así como la evidencia de su implementación en el tratamiento auditado.
Formatos de autorización de roles para el acceso en sistemas informáticos, así como la evidencia de su implementación en el tratamiento auditado.
Instructivo operativo de controles de seguridad.
Programa de Trabajo de Control Interno.
Plan de monitoreo periódico de medidas de seguridad, así como la evidencia de su implementación en el tratamiento auditado.
Registros de las revisiones realizas por el enlace de protección de datos personales.
Registros de la auditoría integral realizada.
Reporte del estado del sistema de control interno (apartado datos personales). Bitácora para el registro de vulneraciones de seguridad ocurridas.
Procedimiento para la gestión de acciones preventivas y correctivas, así como la evidencia de su implementación en el tratamiento auditado.
Registros de las acciones preventivas y correctivas implementadas como resultado de la auditoría integral o de una vulneración de datos personales ocurrida.
Medidas para medir la efectividad y calidad de la capacitación: • listas de asistencia • constancias de capacitación • material de la capacitación impartida • cursos internos como externos

III. Conclusión y cierre de auditoría voluntaria

Cédulas de conclusiones

En las cédulas de conclusiones se asientan y desarrollan los rubros siguientes:

Contenido
Principio, deber u obligación revisada.
Nombre del responsable que solicitó la auditoría voluntaria.
Número de expediente de auditoría voluntaria.
Área auditada.
Día, mes, año de elaboración.
Proceso o tratamiento auditado.
Descripción del fundamento de la obligación.
Describir la obligación revisada.
Marcar con X en caso de ser una conformidad.
Marcar con X en caso de ser una no conformidad.
Realizar descripción de la conformidad o no conformidad.
Descripción de la acción correctiva, en su caso.
Nombre y cargo de la persona servidora pública que funge como auditor líder.
Nombre y cargo de la persona servidora pública que realizó la cédula de conclusiones.

Acuerdo de reunión de cierre de auditoría voluntaria

Una vez que se hayan elaborado las cédulas de conclusiones, la DGPAR previo acuerdo que lleve a cabo con el sujeto obligado fijar fecha para desahogar la reunión de cierre de auditoría voluntaria, elaborará un acuerdo de reunión de cierre para que comparezca el sujeto obligado al Instituto.

Reunión de cierre de auditoría voluntaria

La reunión de cierre deberá llevarse a cabo para presentar los hallazgos y las conclusiones de la auditoría. Entre los participantes en la reunión de cierre debería incluirse, además del equipo auditor, a los representantes del responsable auditado que se hayan señalado.

En su caso, la persona servidora pública que funge como líder del equipo auditor tendrá que señalar al responsable solicitante las situaciones encontradas durante la auditarla voluntaria que pudieran constituir un riesgo en el tratamiento de datos personales que efectúa el área auditada.

La reunión consistirá en la comunicación de los hallazgos de la auditoría y las conclusiones de la misma, en virtud de que el informe final será notificado posteriormente al responsable solicitante.

Cualquier opinión divergente relativa a los hallazgos de la auditoría o las conclusiones entre las personas integrantes del equipo auditor y el responsable auditado tendrá que discutirse entre las partes y, de ser posible, resolverse. Si no se resuelve, deberán registrarse todas las opiniones en el acta correspondiente. Al finalizar la reunión de cierre se deberá suscribirse un acta.

¿Qué contenido lleva el acta de cierre de auditoría?

El acta de cierre de auditoría deberá contener al menos, lo siguiente:

- El lugar, fecha y hora de realización de reunión de cierre.
- La denominación del responsable solicitante.
- Los nombres completos, cargos y firmas de todas las personas servidoras públicas y personas que intervinieron.
- La narración de los hechos ocurridos durante la reunión de cierre de auditoría voluntaria, y

Informe final. La DGPAR deberá elaborar el proyecto de informe final, para que éste sea emitido con posterioridad por la Secretaría de Protección de Datos Personales del INAI. Además de describir el contexto general de la auditoría voluntaria practicada, entre ello, sus objetivos, alcance, datos generales del equipo auditor y el responsable solicitante, los hallazgos y evidencias: el informe final deberá:

- Señalar los resultados obtenidos de la auditoria, pronunciándose sobre la conformidad o no conformidad de los controles, mecanismos o procedimientos adoptados por el responsable solicitante, que fueron auditados, para el cumplimiento de las obligaciones establecidas en la Ley General, los Lineamientos Generales y demás normatividad que resulte aplicable, y
- Orientar al responsable sobre el fortalecimiento y un mejor cumplimiento de las obligaciones previstas en la Ley General, los Lineamientos Generales y cualquier normatividad que resulte aplicable, señalando las medidas, acciones y sugerencias específicas, de carácter preventivo y/o correctivo, en función de las características generales y particulares del tratamiento de datos personales y los hallazgos obtenidos en la auditoría voluntaria.

El informe final se elabora en dos tantos originales, de los cuales uno se entrega al responsable solicitante con copia simple de las cédulas de conclusiones firmadas, mientras que el otro tanto se utiliza como acuse de recibo y se integra al expediente que corresponda, junto con los originales de las cédulas de conclusiones.

El informe final de la auditoría debe ser notificado al responsable auditado dentro de los cinco días siguientes contados a partir de su emisión.

Seguimiento de no conformidades de auditoría voluntaria

Acuerdo de requerimiento de evidencia para dar cumplimiento a las no conformidades

El Instituto podrá pedir al responsable auditado que informe sobre la implementación de las recomendaciones que hayan sido emitidas en el informe final de la auditoría conforme a los términos y plazos establecidos en el mismo informe.

Cédulas de seguimiento

En las cédulas de seguimiento el equipo auditor analiza la evidencia remitida por la parte auditada a efecto de concluir si las no

conformidades han sido solventadas o no solventadas, se integran con el siguiente contenido:

Contenido
Principio, deber u obligación revisados.
Nombre del responsable que solicitó la auditoría voluntaria.
Número de expediente de auditoría voluntaria.
Área auditada.
Día, mes y año de elaboración.
Proceso o tratamiento auditado.
Descripción del fundamento de la obligación.
Describir la obligación revisada.
Marcar con X en caso de ser una conformidad.
Marcar con X en caso de ser una no conformidad.
Realizar descripción de la no conformidad.
Descripción de la acción correctiva emitida.
Descripción de la atención del hallazgo por el responsable.
Resultado de la revisión, derivado de la atención de hallazgos.
Nombre y cargo de la persona servidora pública que funge como auditor líder.
Nombre y cargo de las personas servidoras públicas integrantes del equipo auditor.

Acuerdo de finalización de expediente

Una vez concluida la totalidad de actividades de la auditoría voluntaria, la SPDP instruye a la DGPAR para que elabore el acuerdo de finalización de expediente correspondiente, el cual será suscrito por la primera de las citadas.

inai

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales