UNMSM
Fundación
SAN MARCOS
Por el desarrollo de la Ciencia y la Cultura

DIPLOMADO DE ESPECIALIZACIÓN

GESTIÓN DE LA CIBERSEGURIDAD Y PRIVACIDAD

RESUMEN EJECUTIVO

GUÍA DE AUDITORIAS VOLUNTARIAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

JULIO – OCTUBRE 2026

CENCAEP
CAPACITA

RESUMEN EJECUTIVO

Guía de Auditorías Voluntarias en materia de Protección de Datos Personales para el Sector Público

Enfoque ejecutivo, de cumplimiento, privacidad y seguridad de la información

Documento base: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), México — agosto de 2023

1. Resumen ejecutivo

La Guía presenta un modelo práctico para que los sujetos obligados del sector público federal mexicano evalúen, de manera voluntaria, el nivel de adecuación y eficacia de sus controles de protección de datos personales. La auditoría se concibe como un proceso sistemático, independiente y documentado, orientado a obtener evidencia sobre el cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, sus Lineamientos Generales y demás normativa aplicable.

Su valor principal radica en el enfoque preventivo: la auditoría no busca sancionar, sino identificar brechas, debilidades de control y oportunidades de mejora antes de que se materialicen incumplimientos o incidentes. El resultado se expresa en conformidades y no conformidades, acompañado de acciones correctivas, preventivas y recomendaciones que permiten fortalecer la gobernanza de privacidad y la seguridad del tratamiento.

Desde una perspectiva de ciberseguridad, la Guía trasciende el cumplimiento formal. Exige demostrar que las medidas de seguridad están efectivamente implementadas mediante evidencia verificable: inventarios, análisis de riesgos y brechas, controles de acceso, monitoreo, continuidad del negocio, recuperación ante desastres, bitácoras de vulneraciones, capacitación y mecanismos de mejora continua.

2. Propósito, fundamento y alcance

La publicación busca facilitar la comprensión de la naturaleza, alcance, procedimiento y beneficios de las auditorías voluntarias que realiza el INAI. Su fundamento central se encuentra en el artículo 151 de la Ley General, que permite a los responsables someterse voluntariamente a auditorías destinadas a verificar la adaptación, adecuación y eficacia de controles, medidas y mecanismos de protección de datos. Los Lineamientos Generales desarrollan las reglas del procedimiento y el Manual de auditorías voluntarias establece requisitos, condiciones y etapas operativas.

- El alcance puede ser parcial, limitado a determinados principios, deberes u obligaciones, o total.
- Debe delimitar el área, tratamiento o proceso, finalidades, tipos de datos, titulares, transferencias, medidas de seguridad, tecnología y periodo evaluado.
- Los criterios de auditoría se integran por la Ley General, los Lineamientos, la normativa aplicable y las políticas, procedimientos o manuales internos pertinentes.

3. Características esenciales de la auditoría

Elemento	Contenido ejecutivo

Naturaleza	Proceso sistemático, independiente y documentado, iniciado a solicitud del responsable.
Finalidad	Evaluar la adaptación, adecuación y eficacia de controles, medidas y mecanismos aplicados al tratamiento de datos personales.
Enfoque	Preventivo y no punitivo; los resultados de la auditoría voluntaria no dan lugar, por sí mismos, al inicio de un procedimiento de verificación o sancionatorio.
Duración	50 días contados desde el día siguiente a la fecha fijada en el acuerdo de inicio; puede ampliarse una sola vez por un periodo igual cuando exista justificación.
Ejecución	Revisión documental y, cuando corresponda, revisión en sitio.
Resultado	Informe final con conformidades, no conformidades y medidas de fortalecimiento; puede existir seguimiento posterior.

4. Actores y responsabilidades

El equipo auditor está integrado por personas servidoras públicas adscritas a la unidad competente del INAI y puede contar con expertos técnicos. Debe actuar con legalidad, honradez, lealtad, imparcialidad, eficiencia, profesionalismo, objetividad, transparencia, integridad, reserva y confidencialidad, manteniendo independencia de criterio.

El responsable auditado debe proporcionar la información y documentación vinculada con el tratamiento, permitir el acceso a registros, archivos, sistemas, equipos y demás medios de tratamiento, y facilitar el ingreso a las instalaciones donde se realiza el tratamiento. La Guía enfatiza que, dentro del procedimiento, no puede negarse el acceso a la información relacionada con el objeto auditado invocando reserva o confidencialidad.

5. Procedimiento de auditoría voluntaria

El procedimiento se estructura en cuatro fases encadenadas:

1. Preparación e inicio de la auditoría voluntaria.
2. Desarrollo de la auditoría.
3. Conclusión y cierre.
4. Seguimiento de no conformidades, cuando corresponda.

5.1 Preparación e inicio

La solicitud debe identificar al responsable y su domicilio, personas autorizadas para notificaciones, área a cargo del tratamiento y descripción del tratamiento a auditar. Esta descripción comprende finalidades, tipos de datos, categorías de titulares, transferencias, medidas de seguridad, tecnología utilizada y cualquier información relevante. También debe exponer las razones para solicitar la auditoría e identificar y firmar a la autoridad facultada.

Antes de admitir la solicitud, se verifica que no exista una denuncia, procedimiento de verificación o verificación de oficio relacionada con el mismo o similar tratamiento, y que el INAI sea competente. La solicitud puede desecharse por improcedencia, duplicidad, falta de competencia, porque el área no pertenezca al responsable, porque la materia no sea protección de datos personales o por no atender una prevención dentro del plazo concedido.

Si la solicitud es incompleta o poco clara, puede emitirse una prevención. El responsable dispone de un máximo de diez días para subsanar las omisiones. Admitida la solicitud, se desarrolla una reunión preparatoria para precisar objetivos y alcance y dejar constancia de los acuerdos.

5.2 Desarrollo: acuerdo de inicio y obtención de evidencia

El acuerdo de inicio identifica la fecha, auditor líder, objetivos, alcance, criterios, representante del responsable, aspectos de confidencialidad y seguridad de la información y los requerimientos documentales. Durante cualquier fase puede solicitarse información adicional vinculada con el tratamiento auditado.

La revisión documental contrasta políticas, programas, procedimientos y prácticas con los criterios aplicables. La revisión en sitio verifica que la operación real coincida con lo documentado. Cuando se efectúa una visita, la orden debe precisar objetivos, alcance, personal auditor, unidad administrativa, fecha, recursos requeridos y consideraciones de seguridad o clasificación de información; además, se levanta el acta correspondiente.

6. Qué se audita: principios de protección de datos

Principio	Foco de auditoría
Licitud	Existencia de base normativa para el

	tratamiento y coherencia con el aviso de privacidad, documento de seguridad y programa de protección de datos.
Finalidad	Finalidades concretas, lícitas, explícitas y legítimas, vinculadas con las atribuciones de la unidad administrativa.
Lealtad	Tratamiento transparente y consistente con la información proporcionada a la persona titular; se consideran también resultados de revisiones previas.
Consentimiento	Mecanismos para obtener, documentar y revocar el consentimiento cuando corresponda, incluido el tratamiento directo o indirecto y reglas de representación.
Calidad	Mecanismos para mantener datos exactos, completos y actualizados, así como conservación, bloqueo y supresión.
Proporcionalidad	Minimización: datos adecuados, relevantes y estrictamente necesarios para cada finalidad.
Información	Avisos de privacidad integral y simplificado, mecanismos de puesta a disposición y claridad de las solicitudes de consentimiento.
Responsabilidad	Recursos, políticas, programas, capacitación, supervisión, atención de dudas y quejas y, cuando aplique, privacidad por diseño.

7. Otras obligaciones relevantes

- Derechos ARCO: procedimientos, medios, formatos, guías, acreditación de identidad y evidencias de atención.
- Comité de Transparencia: existencia, programa de trabajo, supervisión del documento de seguridad y capacitación.
- Unidad de Transparencia: procedimientos internos para gestionar derechos ARCO y mecanismos de evaluación de calidad.

- Portabilidad: documentación generada para atender solicitudes de portabilidad conforme a los parámetros aplicables.
- Relación responsable–encargado y cómputo en la nube: contratos, cláusulas, convenios, avisos de privacidad y consentimiento, según corresponda.
- Transferencias: instrumentos jurídicos, comunicación del aviso de privacidad, consentimiento y procedimiento de comunicación al receptor.

8. Deberes de confidencialidad y seguridad

El componente de seguridad es uno de los apartados de mayor relevancia técnica. La auditoría no se limita a comprobar la existencia de documentos; busca evidencia de que los controles operan en el tratamiento evaluado.

- Controles de confidencialidad y evidencia de su implementación, incluidos convenios, contratos y responsivas.
- Documento de seguridad y evidencia de aplicación efectiva.
- Inventario de datos personales y sistemas de tratamiento.
- Definición de funciones y obligaciones del personal que trata datos personales.
- Análisis de riesgos y análisis de brecha.
- Plan de trabajo para atender brechas y fortalecer controles.
- Mecanismos de monitoreo y revisión de medidas de seguridad.
- Programa general de capacitación y evidencias de efectividad.
- Mapas, diagramas, capturas y documentación de infraestructura tecnológica: servidores, routers, dispositivos y sistemas relacionados.
- Catálogo de medios y ubicaciones físicas o electrónicas de almacenamiento.
- Plan de continuidad del negocio y plan de recuperación ante desastres.
- Autorización de roles y accesos a sistemas, con evidencia de implementación.
- Bitácora de vulneraciones de seguridad y procedimientos de acciones preventivas y correctivas.

En términos de gestión de riesgos, este conjunto de evidencias permite evaluar no solo la existencia del control, sino su trazabilidad, operación y capacidad para reducir riesgos sobre la confidencialidad, integridad y disponibilidad de la información personal. La combinación de inventario, análisis de riesgos, brechas, monitoreo, continuidad y registro de vulneraciones constituye una base sólida para una gestión de seguridad orientada a evidencia.

9. Papeles de trabajo, hallazgos y criterios de evaluación

Las listas de comprobación constituyen papeles de trabajo del equipo auditor. Registran el responsable, área y tratamiento auditados, normativa y disposición revisada, expediente, fecha y horario, principio/deber/obligación, comprobación de adecuación, evidencia presentada y responsables de la revisión. Los documentos sugeridos por la Guía son ejemplos orientativos y no una lista cerrada de cumplimiento.

Un hallazgo surge de contrastar la evidencia recopilada con el objetivo, alcance y criterios definidos. Existe conformidad cuando los controles, mecanismos o procedimientos son adecuados para cumplir las obligaciones; existe no conformidad cuando resultan inadecuados. Esta distinción es central porque

conecta la evaluación con acciones correctivas, preventivas y recomendaciones concretas.

10. Conclusión, cierre e informe final

Las cédulas de conclusiones documentan por cada principio, deber u obligación el fundamento, la obligación revisada, la conformidad o no conformidad y, cuando corresponda, la acción correctiva. Posteriormente se celebra una reunión de cierre para comunicar hallazgos y conclusiones. Las discrepancias deben discutirse y, si no se resuelven, quedar registradas en el acta de cierre.

El informe final presenta el contexto, objetivos, alcance, equipo auditor, responsable, hallazgos y evidencias. Debe pronunciarse sobre la conformidad o no conformidad de los controles auditados y orientar al responsable mediante medidas, acciones y sugerencias preventivas o correctivas. La Guía establece que el informe debe notificarse dentro de los cinco días siguientes a su emisión.

11. Seguimiento de no conformidades

El Instituto puede requerir evidencia sobre la implementación de las recomendaciones formuladas. Las cédulas de seguimiento registran la no conformidad, la acción correctiva, la respuesta del responsable y el resultado de la revisión, permitiendo determinar si el hallazgo fue solventado o permanece pendiente. Concluidas las actividades, se emite el acuerdo de finalización del expediente.

12. Lectura ejecutiva desde la ciberseguridad

Dimensión	Riesgo que se controla	Evidencia clave
Gobernanza	Controles aislados o sin responsables claros	Políticas, programa, roles, supervisión y recursos.
Datos	Desconocimiento de qué información se trata y dónde reside	Inventario de datos, sistemas y ubicaciones.
Riesgo	Medidas no alineadas con amenazas y exposición real	Análisis de riesgos, brecha y plan de trabajo.
Acceso	Uso o consulta no autorizada	Roles, autorizaciones y controles de acceso.
Resiliencia	Interrupción o pérdida de información	Continuidad del negocio y recuperación ante desastres.
Incidentes	Falta de trazabilidad y respuesta	Bitácora de vulneraciones y acciones

		correctivas/preventivas.
Personas	Errores humanos y desconocimiento normativo	Capacitación, constancias y medición de efectividad.
Terceros	Tratamientos sin garantías suficientes	Contratos, cláusulas, convenios y controles sobre encargados.

13. Conclusiones ejecutivas

- La auditoría voluntaria es una herramienta de aseguramiento preventivo que permite evaluar la eficacia real del sistema de protección de datos antes de que una debilidad se convierta en incumplimiento o incidente.
- La calidad de la auditoría depende de evidencia objetiva. Tener políticas o procedimientos no es suficiente: debe acreditarse su implementación, seguimiento y eficacia.
- El alcance debe definirse con precisión. Una delimitación clara del tratamiento, área, datos, titulares, tecnología y controles evita revisiones dispersas y mejora la utilidad de los hallazgos.
- La seguridad de los datos personales requiere un enfoque basado en riesgos que integre inventarios, análisis de riesgos y brechas, control de accesos, monitoreo, continuidad, recuperación, gestión de vulneraciones y capacitación.
- El seguimiento convierte el informe en mejora continua: las no conformidades deben traducirse en acciones verificables y evidencia de cierre.

Nota de alcance

Este resumen sintetiza exclusivamente el contenido de la Guía del INAI. Aunque el documento fuente ya se encuentra redactado en español, se ha reformulado en español ejecutivo y técnico, preservando su sentido jurídico y operativo. Las referencias institucionales y normativas corresponden al marco mexicano descrito en la publicación y no deben interpretarse automáticamente como obligaciones aplicables a otras jurisdicciones.