Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia

ÍNDICE

I. Presentación 1
II. Marco jurídico 3
III. Justificación metodológica 4
IV. Disposiciones generales 5
V. Reglas generales de evaluación 15
VI. Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia 24
Capítulo I. Metodología 24
A) De las vertientes, variables, formatos y criterios 26
Capítulo II. Criterios y formatos 27
Vertiente 1: Principios 29
Variable 1.1: Aviso de privacidad integral 29
Variable 1.2: Mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones de la Ley General y demás disposiciones aplicables. 33
Vertiente 2: Deberes 37
Variable 2.1: Deber de seguridad 37
Variable 2.2: Deber de confidencialidad y comunicaciones de datos personales 53
Vertiente 3: Ejercicio de los derechos ARCO 61
Variable 3.1: Mecanismos para el ejercicio de los derechos ARCO 61
Vertiente 4: Portabilidad 68
Variable 4.1: Portabilidad de datos personales 68
Vertiente 5: Acciones preventivas en materia de protección de datos personales 73
Variable 5.1: Evaluación de impacto en la protección de datos personales 73
Vertiente 6: Responsables en materia de Protección de Datos Personales 79
Variable 6.1: El Comité de Transparencia y la Unidad de Transparencia 79
Variable 6.2: Oficial de Protección de Datos Personales 82
Capítulo III. Indicadores 85
VII. Anexos 91
Anexo 1. Anexo- Guía 1. Información sobre el aviso o los avisos de privacidad integrales. 91
Anexo 2. Anexo- Guía 2. Instrumentos jurídicos que regulan la relación con los encargados con cláusula general de guardar confidencialidad. 91
Anexo 3. Anexo- Guía 3. Instrumentos jurídicos mediante los cuales se formaliza la contratación o adhesión a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias. 91
Anexo 4. Anexo- Guía 4. Trasferencias de datos personales. 92
Anexo 5. Anexo- Guía 5. Información sobre derechos ARCO. 92
Anexo 6. Anexo- Guía 6. Avisos de privacidad portabilidad. 92
Anexo 7. Fichas técnicas e indicadores. 92
Anexo 8. Formatos obligatorios para publicación de medios de verificación. 92

I. Presentación

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), como organismo constitucional autónomo y especializado, responsable de garantizar el cumplimiento del derecho fundamental a la protección de datos personales en posesión de los sujetos obligados, se rige por lo dispuesto en el artículo 6°, Base A, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos; y en observancia de lo que dispone el artículo 16, párrafo segundo del mismo ordenamiento, respecto del cual se prevé que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos así como a manifestar su oposición, en los términos que fije la ley; la cual establece los supuestos de excepción a los principios que rigen el tratamiento de datos, ya sea por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas, o para proteger los derechos de terceros.

En este sentido, por mandato constitucional se dispone que este organismo garante se regirá, en materia de protección de datos personales en posesión de sujetos obligados, en los términos que determine la ley general emitida por el Congreso de la Unión.

Debido a lo anterior, el 26 de enero de 2017, se publicó en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General), la cual tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho de toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

La Ley General dispone obligaciones concretas para que cada responsable del tratamiento de datos personales cumpla con los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales; los cuales deberán sujetarse a las facultades o atribuciones que la normatividad aplicable les confiera.

Asimismo, establece que todo tratamiento de datos personales que efectúen los responsables deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas; sin que el responsable pueda obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

En este contexto, en el artículo 89 fracciones I, XIX y XXV de la Ley General, se establecen para el INAI, entre otras, las atribuciones de garantizar el ejercicio del derecho a la protección de datos personales en posesión de sujetos obligados; emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general para el debido cumplimiento de los principios, deberes y obligaciones que establece la Ley General, así como para el ejercicio de los derechos de los titulares;

así como de diseñar y aplicar indicadores y criterios para evaluar el desempeño de los responsables respecto al cumplimiento de la Ley General y demás disposiciones que resulten aplicables en la materia.

Por lo anterior, y con la finalidad de observar lo dispuesto por el artículo 89 fracción XXV de la Ley General, 246 y 248 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales); el presente documento integra una perspectiva metodológica y conceptual que consiste en el establecimiento de la metodología, criterios, formatos e indicadores necesarios para evaluar el desempeño de los responsables respecto del cumplimiento de las disposiciones que se establecen en la Ley General, y demás disposiciones aplicables en la materia.

II. Marco jurídico

El presente documento tiene como base las disposiciones contenidas en los siguientes ordenamientos:

I. Constitución Política de los Estados Unidos Mexicanos;

II. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

III. Ley General de Transparencia y Acceso a la Información Pública;

IV. Ley Federal de Transparencia y Acceso a la Información Pública;

V. Lineamientos Generales de Protección de Datos Personales para el Sector Público;

VI. Lineamientos que establecen los Parámetros, Modalidades y Procedimientos para la Portabilidad de Datos Personales;

VII. Disposiciones Administrativas de carácter general para la elaboración, presentación y valoración de Evaluaciones de Impacto en la Protección de Datos Personales;

VIII. Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

IX. Acuerdo mediante el cual se emiten las recomendaciones en materia de acceso a la información y datos personales ante cambios de Titulares de Unidad de Transparencia, de Comité de Transparencia y de Servidores Públicos a cargo el tratamiento de datos personales;

X. Acuerdo mediante el cual el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, aprueba el Padrón de sujetos obligados del ámbito federal, en términos de la Ley General de Transparencia y Acceso a la Información Pública, y

XI. Acuerdo mediante el cual se aprueba que el Padrón de sujetos obligados del ámbito federal, en términos de la Ley General de Transparencia y Acceso a la Información Pública y sus respectivas actualizaciones llevadas a cabo por la Secretaría de Acceso a la Información, se utilice como referencia directa del catálogo de sujetos obligados en el ámbito federal para efectos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

III. Justificación metodológica

La metodología plasmada en el presente documento mediante la cual la Dirección General de Evaluación Investigación y Verificación del Sector Público (DGEIVSP) evaluará el desempeño de los responsables en el cumplimiento de la Ley General, y demás disposiciones aplicables en la materia, tiene un enfoque cuantitativo, cuya finalidad consiste en realizar una medición general, objetiva, imparcial y equitativa de cada uno de los responsables evaluados, respecto del citado cumplimiento normativo.

Esta metodología permitirá al INAI ejercer y cumplir las atribuciones y funciones en materia de evaluación del desempeño establecidas en los artículos 89, fracción XXV de la Ley General; 246, 247, 248, 249, 250, 251, 252 y 253 de los Lineamientos Generales ; 25 fracción XXVIII y 41 Bis, fracciones XII, XIII, XIV, XV, XVI y XVII del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Estatuto Orgánico), con lo cual será viable evaluar el quehacer general de los responsables respecto de los principios, deberes y obligaciones establecidas en la Ley de la materia, sin que ello signifique realizar una valoración cualitativa del contenido específico de los documentos evaluados, en virtud de que las atribuciones de verificación y vigilancia establecidas en los artículos 89 fracción VI, XI, XIV, XVII y XXXV; 146, 147 y 151, de la Ley General, así como los artículos 25, fracciones XIV y XVII; 41 Bis, fracciones I, II, II, IV, y VI y 45, fracción IV, del Estatuto Orgánico, obedecen a facultades diversas a las de evaluación del desempeño.

Con base en lo anterior, a través de la ejecución de la presente evaluación cuantitativa, será posible valorar numéricamente mediante el método binario, el cumplimiento general de la Ley General y demás disposiciones aplicables en la materia, a cargo de cada responsable evaluado.

Los resultados finales de las evaluaciones del desempeño de cada sujeto obligado, así como del conjunto de ellos, será expresado en índices (porcentajes) simples y globales obtenidos de acuerdo con la metodología, criterios, formatos e indicadores que se exponen en el presente documento.

IV. Disposiciones generales

Primero. El presente documento es de observancia obligatoria para los sujetos obligados del ámbito federal a que se refiere el artículo 1 de la Ley General, de conformidad con lo dispuesto en el artículo 248 de los Lineamientos Generales; tiene como objetivo establecer la metodología, criterios, formatos e indicadores mediante los cuales los responsables serán evaluados, así como los medios de verificación a través de los que deberán acreditar el cumplimiento de las disposiciones establecidas en la Ley General, y demás disposiciones aplicables en la materia; y con ello, el INAI esté en posibilidad de ejercer y cumplir sus atribuciones en materia de evaluación del desempeño; de conformidad con lo dispuesto en los artículos 89, fracción XXV de la Ley General; 246, 247, 248, 249, 250, 251, 252 y 253 de los Lineamientos Generales; 25 fracción XXVIII, y 41 Bis, fracciones XII, XIII, XIV, XV, XVI y XVII del Estatuto Orgánico.

Segundo. De conformidad con lo dispuesto en los artículos 16 de la Ley General y 7 de los Lineamientos Generales, en todo tratamiento de datos personales, el responsable deberá observar los siguientes principios rectores:

I. Licitud
II. Finalidad
III. Lealtad
IV. Consentimiento
V. Calidad
VI. Proporcionalidad
VII. Información
VIII. Responsabilidad

Tercero. Considerando las definiciones establecidas en la Ley General y en los Lineamientos Generales, así como en las demás previstas en la normatividad aplicable en la materia, y aquella utilizada en los instrumentos técnicos para la evaluación; para los efectos del presente documento, se entenderá por:

I. Anexo-Guía: Instrumento que sirve de apoyo o ejemplo, a los responsables para integrar la información y los documentos que serán utilizados como medios de verificación del

cumplimiento de sus obligaciones, así como para identificar que éstos cumplan con lo establecido en el presente documento técnico;

II. **Apartado virtual de Protección de datos personales:** El apartado a que se refiere el artículo 250 de los Lineamientos Generales, el cual sirve a los responsables como medio para acreditar el cumplimiento de sus obligaciones en materia de protección de datos personales, así como para rendir cuentas a las personas titulares y al Instituto sobre el tratamiento de los datos personales en su posesión permitiendo evaluar el cumplimiento de los principios, deberes y obligaciones; siendo además repositorio de los medios de verificación documentales que serán utilizados en los ejercicios de evaluación;

III. **Áreas:** Instancias de los sujetos obligados previstas en sus respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales. La denominación de las áreas que los sujetos obligados publiquen deberá corresponder a la denominación establecida en su estructura orgánica aprobada y sin utilizar siglas o abreviaturas;

IV. **Asesorías técnicas:** Asistencia técnica del Instituto dirigida a los responsables, para la implementación y cumplimiento de los criterios e indicadores previstos en los instrumentos técnicos de evaluación, señalados en el artículo 253 de los Lineamientos Generales;

V. **Autorización de excepción de cumplimiento:** Documento a través del cual el Instituto autoriza al responsable solicitante durante la evaluación vinculante, la no observancia del cumplimiento de uno o varios criterios establecidos en el presente documento. Dicha autorización, únicamente tendrá vigencia durante el periodo de evaluación que se está informando;

VI. **Aviso de privacidad:** Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;

VII. **Base(s) 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;

VIII. **Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles

responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;

IX. Caso fortuito o de fuerza mayor. Situación en la que el incumplimiento de las disposiciones establecidas en el presente documento no es imputable al responsable, siempre que cuente con la autorización de excepción de cumplimiento respectiva; toda vez que se ve impedido a cumplir a causa de un acontecimiento que está fuera de su dominio o de su voluntad. Se pueden distinguir tres categorías de acontecimientos constitutivos del caso fortuito o de fuerza mayor: 1) Los que provengan de actos de la naturaleza, 2) Hechos derivados del ser humano, y 3) Los derivados de actos de la autoridad. Cuando se presenta alguno de ellos, el responsable debe presentar solicitud de excepción de cumplimiento a la Dirección General de Evaluación, Investigación y Verificación del Sector Público del INAI, con la finalidad de que resuelva sobre su procedencia;

X. Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública;

XI. Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;

XII. Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;

XIII. Criterio: Parámetro para calificar las características específicas de la información publicada en cada una de las variables evaluadas. Los criterios se usan para determinar el valor ordinal de las variables. El valor de la variable dependerá de las características identificadas en la información; cuantas más características se reconozcan, mayor es el valor ordinal de la variable;

XIV. 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;

XV. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para

éste. De manera enunciativa más no limitativa, se consideran sensibles los 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;

XVI. Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales señalados en la Ley General;

XVII. Días: Se entenderán días hábiles, salvo mención expresa a días naturales;

XVIII. Dictamen de medición de cumplimiento. Documento que pone fin al procedimiento de evaluación, mediante el cual se establece el resultado de la evaluación del desempeño de carácter vinculante a los responsables. Este documento contiene el índice general de cumplimiento del responsable, señala las recomendaciones de carácter particular que fueron subsanadas dentro del periodo de 20 días hábiles dispuesto en el artículo 251 de los Lineamientos Generales, así como las que no fueron subsanadas por el responsable, una vez transcurrido el plazo para su atención;

XIX. Disposiciones para las evaluaciones de impacto: Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de Evaluaciones de Impacto en la Protección de Datos Personales;

XX. DGEIVSP: Dirección General de Evaluación, Investigación y Verificación del Sector Público, del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XXI. Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;

XXII. Documento técnico de evaluación: El presente instrumento técnico para la evaluación;

XXIII. 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;

XXIV. Evaluación de tipo diagnóstico: Evaluación realizada a los responsables de conformidad con lo dispuesto en el artículo 246 de los Lineamientos Generales, de la cual se derivan recomendaciones de carácter general respecto del cumplimiento de la Ley General, y

demás disposiciones que resulten aplicables en la materia; las cuales no generan efectos vinculantes en relación con el resultado;

XXV. Evaluación vinculante: Evaluación realizada a los responsables en términos de lo establecido en los artículos 246 y 251 de los Lineamientos Generales, de la cual derivan un Dictamen de medición de cumplimiento y recomendaciones de carácter particular cuya atención es de carácter obligatorio para los responsables, con la finalidad de evitar el incumplimiento de las disposiciones en la materia;

XXVI. Formato: Tablas obligatorias establecidas en cada variable que tienen como objetivo asegurar la organización, presentación y publicación de los criterios y los medios de verificación del cumplimiento de los responsables;

XXVII. Guía y consideraciones para la evaluación: Se refiere a la Guía y consideraciones para la evaluación del desempeño de los responsables respecto del cumplimiento la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones aplicables. Es el documento que sirve de apoyo y orientación al interior de la DGEIVSP para la realización de las evaluaciones del desempeño a que se refiere el artículo 89, fracción XXV de la Ley General;

XXVIII. Herramienta de Evaluación de Protección de Datos Personales (HEPDP): Documento en el cual se registran los datos de identificación y seguimiento de la evaluación del desempeño realizada a cada responsable;

XXIX. Hipervínculo: Elemento electrónico publicado por el responsable, el cual se utiliza para enlazar a la información solicitada en el criterio de evaluación específico;

XXX. Indicador: Herramienta cuantitativa que permite mostrar, a manera de indicios y señales, aspectos relacionados con los logros, avances y cambios que contribuyen a evaluar el desempeño de los responsables en el cumplimiento de la Ley General;

XXXI. Índice global de cumplimiento de criterio (IGCCr): Porcentaje de criterios del Documento Técnico de Evaluación que son cumplidos por el conjunto de sujetos obligados evaluados. Se obtiene promediando los valores de cumplimiento de cada criterio obtenidos por los sujetos obligados evaluados;

XXXII. Índice global de cumplimiento de formato (IGCFo): Porcentaje de criterios contenidos en cada formato del Documento Técnico de Evaluación, que son cumplidos por el conjunto de

sujetos obligados evaluados. Se obtiene promediando los índices simples de cumplimiento de criterios cumplidos en cada formato de los sujetos obligados evaluados;

XXXIII. Índice global de cumplimiento de protección de datos personales (IGCPDP): Porcentaje de criterios contenidos en el Documento Técnico de Evaluación, que son cumplidos por el conjunto de sujetos obligados evaluados. Se obtiene promediando los índices globales de cumplimiento de vertientes de los sujetos obligados evaluados;

XXXIV. Índice global de cumplimiento de variable (IGCVa): Porcentaje de criterios contenidos en cada variable del Documento Técnico de Evaluación que son cumplidos por el conjunto de sujetos obligados evaluados. Se obtiene promediando los índices globales de cumplimiento de formatos de los sujetos obligados evaluados;

XXXV. Índice global de cumplimiento de vertiente (IGCVe): Porcentaje de criterios contenidos en cada vertiente del Documento Técnico de Evaluación que son cumplidos por el conjunto de sujetos obligados evaluados. Se obtiene promediando los índices globales de cumplimiento de variables de los sujetos obligados evaluados;

XXXVI. Índice simple de cumplimiento de formato (ISCFo): Porcentaje de criterios contenidos en cada formato del Documento Técnico de Evaluación que son cumplidos por el sujeto obligado evaluado. Se obtiene promediando el total de criterios cumplidos entre el total de criterios a cumplir en cada formato que conforma una variable;

XXXVII. Índice simple de cumplimiento de variable (ISCVa): Porcentaje de criterios contenidos en cada variable del Documento Técnico de Evaluación que son cumplidos por el sujeto obligado evaluado. Se obtiene promediando los índices de cumplimiento de cada formato que conforma una variable;

XXXVIII. Índice simple de cumplimiento de vertiente (ISCVe): Porcentaje de criterios contenidos en cada vertiente del Documento Técnico de Evaluación que son cumplidos por el sujeto obligado evaluado. Se obtiene promediando los índices simples de cumplimiento de cada variable que conforma una vertiente;

XXXIX. Índice Simple General de Cumplimiento (ISGC): Porcentaje de criterios contenidos en el Documento Técnico de Evaluación que son cumplidos por el sujeto obligado evaluado. Se obtiene promediando los índices simples de cumplimiento de cada vertiente;

XL. Informe anual: Informe anual a que se refiere el artículo 252 de los Lineamientos Generales, el cual contiene los resultados de la evaluación y la medición del desempeño de los

responsables sobre el cumplimiento de la Ley General, así como el reporte sobre el resultado de la o las evaluaciones del desempeño y el seguimiento a las recomendaciones emitidas en relación con la evaluación que corresponda;

XLI. Instituto o INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados;

XLII. Instrumentos técnicos de evaluación: Todos aquellos documentos de índole técnica, aprobados por el Pleno del Instituto, para el ejercicio de la atribución prevista en la fracción XXV del artículo 89 de la Ley General, de conformidad con lo establecido en los artículos 247 y 248 de los Lineamientos Generales;

XLIII. Interoperabilidad: Capacidad de los responsables, transmisor y receptor, para compartir infraestructura y datos personales a través de la conexión de sus respectivos sistemas o plataformas tecnológicas;

XLIV. Ley General: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

XLV. Ley General de Transparencia: Ley General de Transparencia y Acceso a la Información Pública;

XLVI. Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público;

XLVII. Lineamientos de Portabilidad: Lineamientos que establecen los Parámetros, Modalidades y Procedimientos para la Portabilidad de Datos Personales;

XLVIII. Medidas compensatorias: Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;

XLIX. Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

L. Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;

LI. Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a. Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
b. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
c. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
d. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;

LII. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

a. Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
b. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
c. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
d. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

LIII. Medios de verificación: Se refiere a los medios de verificación documentales que se utilizan en los ejercicios de evaluación, cuyas características y contenido se establecen el Documento Técnico de Evaluación y en el Programa Anual de Evaluación, de conformidad con lo dispuesto en el artículo 250 de los Lineamientos Generales. Los medios de verificación constituyen los datos e información generada y registrada por los responsables y publicada en el apartado virtual “Protección de datos personales”. A través de estos, los responsables rinden cuentas a los titulares y al Instituto sobre el tratamiento de los datos personales en su

posesión y permiten evaluar el cumplimiento de los principios, deberes y obligaciones; atendiendo a la obligatoriedad que les corresponde como responsables;

LIV. Padrón de sujetos obligados para efectos de la Ley General: Acuerdo ACT-PUB/13/08/2019.06, mediante el cual se aprueba que el padrón de sujetos obligados del ámbito federal, en términos de la Ley General de Transparencia y Acceso a la Información Pública y sus respectivas actualizaciones llevadas a cabo por la Secretaría de Acceso a la Información, se utilice como referencia directa del catálogo de sujetos obligados en el ámbito federal para efectos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; publicado en el Diario Oficial de la Federación el 29 de agosto de 2019;

LV. Portabilidad de datos personales: Prerrogativa del titular a que se refiere el artículo 57 de la Ley General;

LVI. Programa anual de evaluación: Instrumento a que se refiere el artículo 249 de los Lineamientos Generales, y en el cual se describirán la planeación de los procesos y actividades que deberán realizarse en torno a la evaluación, en el ejercicio de que se trate;

LVII. Recomendaciones de carácter general: Documento que emite la Dirección General de Evaluación, Investigación y Verificación del Sector Público de conformidad con lo establecido en el artículo 246 de los Lineamientos Generales y 41 Bis, fracción XV del Estatuto orgánico del INAI derivado de la evaluación de tipo diagnóstico, en el cual se indica al responsable el, o los criterios del Documento Técnico de Evaluación que no cumple y, se le precisan las medidas, acciones y sugerencias para la debida observancia de la Ley General y demás disposiciones aplicables en la materia;

LVIII. Recomendaciones de carácter particular: Documento de carácter imperativo, que emite la Dirección General de Evaluación, Investigación y Verificación del Sector Público de conformidad con lo establecido en los artículos 246 y 251 de los Lineamientos Generales y 41 Bis, fracción XV del Estatuto orgánico del INAI; derivado de la evaluación vinculante, en la cual se indica al responsable el, o los criterios del Documento Técnico de Evaluación que no cumple y, se le precisan las medidas y acciones a realizar para su debida observancia, las cuales deberá adoptar en el plazo máximo de 20 días hábiles;

LIX. Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;

LX. Responsable: Los sujetos obligados a que se refiere el artículo 1 de la Ley General, que deciden sobre el tratamiento de datos personales;

LXI. Sistema automatizado: Conjunto de recursos, software, hardware e infraestructura utilizada para el tratamiento de datos personales;

LXII. Sistema Nacional o SNT: El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

LXIII. Solicitud de excepción de cumplimiento: Documento que presenta el responsable dirigido a la DGEIVSP, a través del cual solicita la "Autorización de excepción de cumplimiento" de uno o varios criterios establecidos en el presente documento, mediante la exposición y justificación de los motivos y/o circunstancias que imposibilitan su cumplimiento durante el periodo de evaluación que corresponda;

LXIV. Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;

LXV. Titular: La persona física a quien corresponden los datos personales;

LXVI. Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;

LXVII. Transmisión: Toda comunicación de datos personales realizada entre el responsable transmisor y el responsable receptor, a partir de la portabilidad de datos personales. Tratándose de servicios de cómputo en la nube, la comunicación de datos personales de un servicio o aplicación de un responsable a otro;

LXVIII. Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales;

LXIX. Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia;

LXX. Variable: Aspectos específicos de las vertientes, sobre los cuales se establecen los criterios y medios de verificación para que los responsables acrediten el cumplimiento de la Ley General y demás disposiciones aplicables en la materia, y

LXXI. Vertiente: Cada principio, deber u obligación a evaluar para conocer el cumplimiento de la Ley General y demás normativa aplicable en la materia, por parte de los responsables, y de conformidad con las disposiciones establecidas en el presente documento.

V. Reglas generales de evaluación

Primera. Con fundamento en lo dispuesto en el artículo 246 de los Lineamientos Generales, para dar cumplimiento a lo dispuesto en el artículo 89, fracción XXV de la Ley General, la DGEIVSP diseñará y aplicará los indicadores y criterios aprobados por el Pleno del Instituto para evaluar el desempeño de los responsables respecto del cumplimiento de la Ley General, y demás disposiciones que resulten aplicables en la materia.

Las evaluaciones que practique el Instituto podrán ser vinculantes o de tipo diagnóstico; en ambos casos, tendrán por objeto determinar el estado general que guarda el cumplimiento de la Ley General por parte de los responsables.

Se consideran evaluaciones de tipo diagnóstico cuando no generan efectos concretos en relación con el resultado y, en su caso, se emiten recomendaciones de carácter general; por su parte, son consideradas vinculantes, aquellas en las que el resultado de la evaluación pudiera implicar la adopción de recomendaciones de carácter particular por parte del responsable para evitar un incumplimiento a las disposiciones de la Ley General y, una vez concluido el plazo para su atención señalado en el artículo 251 de los Lineamientos Generales, se emitirá el correspondiente Dictamen de medición de cumplimiento, el cual servirá como insumo para la elaboración del Informe anual sobre el desempeño, señalado en el artículo 252 de los Lineamientos Generales.

Segunda. De conformidad con lo dispuesto en el artículo 247 de los Lineamientos Generales, el Instituto aprobará los instrumentos técnicos de evaluación que sean necesarios para medir el desempeño de los responsables respecto al cumplimiento de las obligaciones previstas en la Ley General y demás disposiciones aplicables en la materia; los cuales contemplarán, al menos, el tipo de evaluación, la metodología, los criterios, los formatos y los indicadores que permitan la realización del ejercicio de evaluación que corresponda.

Tercera. Con fundamento en lo dispuesto en el artículo 248 de los Lineamientos Generales, el cumplimiento de las disposiciones contenidas en el presente documento, así como en los demás

instrumentos técnicos de evaluación, es obligatorio para los sujetos obligados del ámbito federal a que se refiere el artículo 1 de la Ley General.

Cuarta. De conformidad con lo dispuesto en el artículo 249 de los Lineamientos Generales, las evaluaciones se realizarán conforme al programa que anualmente apruebe el Pleno del Instituto.
El Programa Anual de Evaluación que corresponda incluirá, al menos lo siguiente:

a) Tipo de la evaluación;
b) Responsables que serán evaluados;
c) Normatividad aplicable;
d) Información por evaluar;
e) Procedimiento de evaluación;
f) Periodo de evaluación;
g) Calendario de evaluación, y, en su caso,
h) Seguimiento al cumplimiento.

Quinta. Con fundamento en lo dispuesto en el artículo 250 de los Lineamientos Generales, los responsables deberán habilitar en su portal de internet, un apartado virtual denominado "Protección de datos personales" el cual deberá contar cuando menos, con el o los avisos de privacidad integrales aplicables a los tratamientos del sujeto obligado, datos de contacto de la Unidad de Transparencia, así como en su caso, Oficial de Protección de Datos, e información relevante en materia de protección de datos personales.
La publicación en dicho apartado podrá servir a los responsables como un medio para acreditar el cumplimiento de sus obligaciones en materia de protección de datos personales, de conformidad con lo dispuesto en los artículos 16, 45, 54, 72, 107 y 118 de los Lineamientos Generales.
El apartado virtual "Protección de datos personales" será el medio idóneo que servirá a los sujetos obligados para rendir cuentas a los titulares y al Instituto sobre el tratamiento de los datos personales en su posesión, permitiendo con ello evaluar el cumplimiento de los principios, deberes y obligaciones; atendiendo a la obligatoriedad que les corresponde como responsables, en términos de lo previsto en los artículos 26, 29 y 30 de la Ley General.
Dicho apartado será repositorio también, de los formatos y documentos que servirán como medios de verificación documentales en los ejercicios de evaluación, cuyas características y contenido se

establecen en el presente documento, así como en los demás instrumentos técnicos de evaluación y en el Programa Anual, respectivamente.

La información contenida en dicho apartado deberá estar disponible de forma permanente y actualizarse conforme lo determinen el presente documento y el resto de los instrumentos técnicos de evaluación.

Sexta. De conformidad con lo dispuesto en el artículo 251 de los Lineamientos Generales, el Instituto informará a los responsables los resultados de la evaluación vinculante que corresponda y podrá emitir recomendaciones de carácter particular respecto de los hallazgos que resulten de la aplicación de los criterios e indicadores, así como establecer el plazo para su aclaración o atención, el cual no podrá rebasar los 20 días hábiles contados a partir del día siguiente de la notificación.

La emisión de recomendaciones no limita las facultades de investigación y verificación del Instituto, cuando se advierta incumplimiento a las disposiciones de la Ley General o los Lineamientos Generales.

Séptima. Con fundamento en el artículo 252 de los Lineamientos Generales, el Pleno del Instituto aprobará anualmente un informe anual con los resultados de la evaluación y la medición del desempeño de los responsables sobre el cumplimiento de la Ley General y demás disposiciones aplicables en la materia, en términos del Programa Anual de Evaluación que corresponda al ejercicio fiscal de que se trate.

El informe anual contendrá el reporte sobre el resultado de la o las evaluaciones del desempeño y el seguimiento a las recomendaciones emitidas en relación con la evaluación que corresponda.

El informe anual deberá aprobarse a más tardar en el primer trimestre del año siguiente sobre el que se realicen la o las evaluaciones y deberá publicarse en la página de Internet del Instituto.

Octava. De conformidad con lo dispuesto en el artículo 253 de los Lineamientos Generales, los responsables podrán solicitar asesoría técnica del Instituto para el cumplimiento de los criterios e indicadores previstos en el presente documento, así como en los demás instrumentos técnicos de evaluación.

Asimismo, el Instituto a través de la DGEIVSP, podrá programar asesorías técnicas dirigidas a orientar a los responsables en la implementación de los criterios e indicadores previstos en el presente Documento y en los demás instrumentos técnicos de evaluación.

Novena. Para efectos de la evaluación a que se refieren el artículo 89, fracción XXV de la Ley General, el Título Décimo de los Lineamientos Generales y los instrumentos técnicos de evaluación; únicamente se tendrá en cuenta la información y/o documentos publicados por el responsable en el apartado virtual "Protección de Datos Personales" de su portal de internet, misma que se presentará mediante los formatos establecidos en el presente documento, **los cuales son un requisito obligatorio e indispensable para realizar la evaluación, por lo que, la falta de estos será considerada como una imposibilidad para realizar la evaluación al responsable del que se trate y, por tanto, un incumplimiento de los criterios que correspondan[1].**

Décima. Los responsables de reciente creación contarán con un periodo de seis meses para publicar en el apartado virtual "Protección de datos personales" de su portal de internet, la información correspondiente a los criterios, formatos e indicadores dispuestos en el presente documento, así como en los demás instrumentos técnicos de evaluación. Dicho periodo se contará a partir de su incorporación al Padrón de sujetos obligados para efectos de la Ley General.

Décimo primera. Los responsables usarán los formatos especificados en cada variable establecidos en el presente documento, los cuales son de carácter obligatorio; con el objetivo de asegurar que la organización, homologación, presentación y publicación de la información y/o documentos solicitados, sea la idónea para que el Instituto evalúe los medios de verificación correspondientes a los criterios.
Los Anexos-Guía establecidos en el presente documento, servirán de apoyo a los responsables para integrar la información y documentos que serán utilizados como medios de verificación para acreditar el cumplimiento de los criterios correspondientes.
Se contemplan, además, las especificaciones necesarias para la homologación en la presentación y publicación de los medios de verificación, asimismo se detallan los criterios mínimos de carácter general, que los responsables deberán observar al publicar la información respecto al tratamiento de datos personales que realizan.

[1] Anexo 8. Formatos obligatorios para publicación de medios de verificación.

Décimo segunda. Toda la información y/o documentos que los responsables pongan a disposición de los titulares y del Instituto en el apartado virtual "Protección de Datos Personales" en atención a los formatos y criterios contenidos en el presente documento y en los demás instrumentos técnicos de evaluación, deberá encontrarse en un formato que permita su reutilización, a excepción de los casos en los que el documento no lo permita, en cuyo caso el responsable deberá manifestarlo expresamente y deberá publicar la información en formato PDF. En ambos supuestos, se considerará que el documento asociado cumple con el criterio correspondiente, siempre que se encuentre en el formato solicitado, sea completamente legible y sin alguna alteración que impida su lectura.

Décimo tercera. Todos los documentos que se pongan a disposición de los titulares y del Instituto en el apartado virtual "Protección de Datos Personales" en atención al presente documento, deberán ser revisados por el responsable a fin de que **en ningún caso se publique información confidencial o reservada.**

Décimo cuarta. La información y documentos publicados como medios de verificación en cada uno de los formatos y criterios invariablemente deberán cumplir con todos los requisitos y características establecidas por la Ley General y demás disposiciones aplicables en la materia. Para el caso de que los medios de verificación posean **información clasificada como confidencial o reservada**, se deberá publicar la versión pública correspondiente elaborada de conformidad con lo determinado en los artículos 106, 107, 108, 109 y demás relativos de la Ley General de Transparencia.

Décimo quinta. Cuando en las evaluaciones vinculantes el responsable no cuente con la información solicitada como medio de verificación en uno o varios criterios, derivado de un caso fortuito o de fuerza mayor, o por tratarse de información que no corresponde a sus facultades; el responsable podrá quedar exceptuado de dar cumplimiento al criterio o criterios respectivos, atendiendo al siguiente procedimiento:

El responsable deberá enviar una solicitud de excepción de cumplimiento emitida por el Titular de su Unidad de Transparencia o en su caso, por el Oficial de Protección de Datos Personales, dirigida a la DGEIVSP y, adjunto a la misma, deberá enviar el acta emitida por su Comité de Transparencia debidamente formalizada y firmada por sus integrantes, en términos de lo establecido en el artículo 64

de la Ley Federal de Transparencia y Acceso a la Información Pública, en la cual se expongan y justifiquen los motivos y/o circunstancias por las que no cuenta con la información solicitada, debiendo señalar de manera precisa si se trata de un caso fortuito o de fuerza mayor, o se trata de información que no corresponde a sus facultades.

Únicamente se recibirá una solicitud por responsable durante todo el procedimiento de evaluación del desempeño del que se trate, y en caso de que la misma no cumpla con los requisitos establecidos en el párrafo anterior, ésta se tendrá por no recibida.

La solicitud de excepción de cumplimiento se tramitará conforme a las siguientes directrices para los siguientes dos supuestos

Supuesto 1. Caso fortuito o de fuerza mayor, o por tratarse de información que no corresponde a las facultades del responsable, que se presenta antes del proceso de evaluación:

I. Dentro de los primeros 5 días hábiles contados a partir del inicio de la evaluación del desempeño vinculante, el responsable deberá presentar mediante oficio o bien, al correo electrónico institucional evalua-datos@inai.org.mx dirigido a la DGEIVSP, la solicitud de excepción de cumplimiento en la cual deberá exponer y justificar los motivos y/o circunstancias por los que se encuentra impedido para cumplir con uno o varios criterios establecidos en el presente documento, durante el periodo de evaluación correspondiente.

II. Dentro de los 10 días hábiles siguientes, contados a partir de la recepción de la solicitud de excepción de cumplimiento, por parte de la DGEIVSP, ésta emitirá la respuesta correspondiente a la solicitud, la cual podrá consistir en la autorización de excepción del cumplimiento, o la negativa de ésta. La respuesta de la DGEIVSP se enviará al responsable mediante oficio o correo electrónico dirigido al Titular de su Unidad de Transparencia u Oficial de Protección de Datos Personales, según corresponda.

    La falta de respuesta por parte de la DGEIVSP, dentro del plazo a que alude el párrafo anterior, se entenderá como una negativa a la autorización de excepción.

III. Si la respuesta emitida por la DGEIVSP consiste en la negativa de excepción al cumplimiento, el sujeto obligado mantendrá vigente la obligación de cumplir con el/los criterio/s en los términos establecidos en el presente documento, para lo cual contará con un periodo máximo de 5 días hábiles, contados a partir de la recepción o envío de la respuesta, según sea el caso, emitida por la DGEIVSP, para publicar la información correspondiente en su apartado virtual “Protección de Datos Personales”; en el supuesto, de que la información no sea

publicada dentro del plazo señalado se considerará como el incumplimiento del, o los criterios, por lo que, el resultado de la evaluación se determinará como "no cumple (0)".

IV. Si la respuesta emitida por la DGEIVSP consiste en la autorización de excepción del cumplimiento, el sujeto obligado cuenta con un periodo de 2 días hábiles contados a partir de la recepción de la autorización, para publicar la misma en su apartado virtual "Protección de Datos Personales", dentro de cada criterio para el cual le haya sido autorizada la excepción de cumplimiento, a fin de que ésta sea considerada durante la evaluación del desempeño correspondiente.

Cabe destacar que la falta de la publicación por parte del responsable de la autorización de excepción del cumplimiento emitida por la DGEIVSP se considerará como el incumplimiento del o los criterios señalados, por lo que se evaluará como "no cumple (0)".

Supuesto 2. Caso fortuito y de fuerza mayor que se presenta durante el proceso de evaluación:

1. Si una vez iniciado el periodo de evaluación, se presenta un caso fortuito y/o de fuerza mayor al responsable que le impide dar cumplimiento, éste deberá presentar dentro de los 5 días hábiles siguientes en que se presentó el caso fortuito o de fuerza mayor, mediante oficio o bien, al correo electrónico institucional evalua-datos@inai.org.mx dirigido a la DGEIVSP, la solicitud de excepción de cumplimiento en la cual deberá exponer y justificar los motivos y/o circunstancias por los que se encuentra impedido para cumplir con uno o varios criterios establecidos en el presente documento, durante el periodo de evaluación correspondiente;
2. Dentro de los 5 días hábiles siguientes, contados a partir de la recepción de la solicitud de excepción de cumplimiento por parte de la DGEIVSP, ésta emitirá la respuesta correspondiente a la solicitud, la cual podrá consistir en la autorización de excepción del cumplimiento, o la negativa de esta. La respuesta de la DGEIVSP se enviará al responsable mediante oficio o correo electrónico dirigido al Titular de su Unidad de Transparencia u Oficial de Protección de Datos Personales, según corresponda;

   La falta de respuesta por parte de la DGEIVSP, dentro del plazo a que alude el párrafo anterior, se entenderá como una negativa a la autorización de excepción.
3. Si la respuesta emitida por la DGEIVSP consiste en la negativa de excepción al cumplimiento, el sujeto obligado mantendrá vigente la obligación de cumplir con el/los criterio/s en los términos establecidos en el presente documento, para lo cual contará con un periodo máximo de 1 día hábil, contado a partir de la recepción de la negativa emitida por la DGEIVSP, para

publicar la información correspondiente en su apartado virtual "Protección de Datos Personales" y, para el caso que no cuente con la información publicada en el plazo señalado se considerará como el incumplimiento del, o los criterios, por lo que se evaluará como "no cumple (0)", y

4. Si la respuesta emitida por la DGEIVSP consiste en la autorización de excepción del cumplimiento, el sujeto obligado cuenta con un periodo de 2 días hábiles contados a partir de la recepción de la autorización, para publicar la misma en su apartado virtual "Protección de Datos Personales", lo cual deberá realizar en cada criterio para el cual le haya sido autorizada la excepción de cumplimiento, a fin de que esta sea considerada durante la evaluación del desempeño correspondiente.

Cuando en las evaluaciones de tipo diagnóstico, el responsable no cuente con la información solicitada derivado de un caso fortuito o de fuerza mayor, o por tratarse de información que no corresponde a sus facultades; este deberá informarlo a través de su Titular de la Unidad de Transparencia o bien, de su Oficial de Protección de Datos Personales, dentro de los primeros 5 días hábiles contados a partir del inicio de la evaluación del desempeño, mediante oficio o bien, al correo electrónico institucional evalua-datos@inai.org.mx dirigido a la DGEIVSP, exponiendo y justificando los motivos y/o circunstancias por las que no cuenta con la información solicitada, debiendo señalar de manera precisa si se trata de un caso fortuito o de fuerza mayor, o se trata de información que no corresponde a sus facultades.

Como resultado de dicha comunicación, la DGEIVSP corroborará la información remitida por el responsable y la excluirá del resultado final de cumplimiento obtenido por este, haciendo la anotación correspondiente en el informe de la evaluación respectivo.

Décimo sexta. De la actualización de la información:

I. Los formatos publicados deberán modificarse de acuerdo con los periodos de actualización establecidos en el presente documento, y en plazos contados a partir de la última actualización registrada en el formato.

II. Los responsables publicarán los formatos correspondientes dentro de los diez días hábiles siguientes a que la información tenga alguna modificación o actualización.

III. El periodo de conservación de la información de cada una de las vertientes está especificado en el apartado correspondiente a cada variable del presente documento. Por lo que, para

efectos de la evaluación será necesario que los responsables conserven únicamente la información que en cada variable se especifica. Sin embargo, se recomienda que el responsable conserve la información publicada por un histórico de al menos dos años.

IV. La información deberá presentarse en los formatos establecidos en el presente documento, mismos que muestran los campos básicos para identificar, entre otros elementos, los medios de verificación correspondientes.

V. En el apartado virtual "Protección de Datos Personales" de los sitios de internet de los sujetos obligados, se deberá incluir el nombre de la vertiente y de la variable de las cuales están publicando los formatos correspondientes. En caso de que, respecto de alguna vertiente o variable, el responsable no genere información se deberá incluir en el criterio correspondiente la autorización de excepción a que se refiere la regla anterior.

Décimo séptima. Para el cumplimiento del presente documento, así como de los demás instrumentos técnicos de evaluación, se sugiere la siguiente distribución de funciones al interior del responsable con la finalidad de facilitar el cumplimiento de los instrumentos técnicos de evaluación; lo anterior, en atención a lo dispuesto en los artículos 83, 84 y 85 de la Ley General, así como 47 y 48 de los Lineamientos Generales:

I. El Comité de Transparencia, a través de la Unidad de Transparencia o unidad administrativa del responsable que realice las funciones establecidas en el artículo 45 de la Ley General de Transparencia requerirá a las áreas de acuerdo con las facultades, competencias y funciones que les correspondan; la información y/o medios de verificación a publicar en el apartado virtual "Protección de Datos Personales", de conformidad con lo dispuesto en el presente instrumento;

II. Las áreas generarán, organizarán, actualizarán y remitirán a la Unidad de Transparencia o unidad administrativa del responsable que realice las funciones establecidas en el artículo 45 de la Ley General de Transparencia, la información y/o documentos requeridos a fin de dar cumplimiento a las disposiciones establecidas en el presente instrumento;

III. El Comité de Transparencia, a través de la Unidad de Transparencia o unidad administrativa del responsable que realice las funciones establecidas en el artículo 45 de la Ley General de Transparencia validará y publicará la información generada, organizada, actualizada y

remitida por las áreas del responsable, en el apartado virtual "Protección de Datos Personales", y

IV. La Unidad de Transparencia asesorará a las áreas adscritas al responsable en materia de protección de datos personales y, por tanto, en la integración de la información y/o medios de verificación que éstas remitirán para dar cumplimiento a los formatos, criterios e indicadores establecidos en el presente documento.

VI. Metodología, criterios, formatos e indicadores en materia de evaluación del desempeño de los responsables respecto al cumplimiento de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y demás disposiciones que resulten aplicables en la materia

Capítulo I. Metodología

La metodología utilizada en el presente documento se compone de una base que facilita la comparación de sus resultados a través de cada una de las ocasiones en las que sea aplicada.

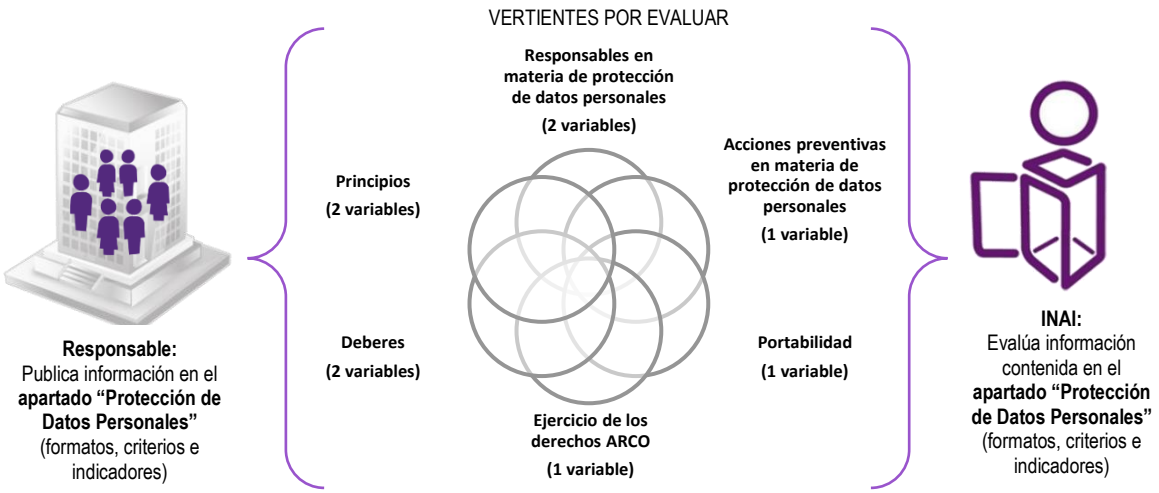
Los elementos que la componen se derivan de las disposiciones establecidas en la Ley General y demás que resulten aplicables en la materia.

La metodología de evaluación utilizada se integra por un componente (normativo – práctico); del cual se desprenden 6 vertientes, 9 variables, 10 formatos y 41 criterios[2]; cuyo cumplimiento será evaluado a partir del número de criterios cumplidos por responsable.

Asimismo, la presente metodología es de carácter inclusivo, toda vez que consiste en la intervención del INAI en su carácter de evaluador, y de los responsables, en su carácter de sujetos obligados evaluados (encargados de la generación y publicación de la información).

Durante la evaluación, el INAI llevará a cabo una revisión de la información en materia de protección de datos personales generada por cada responsable y publicada en el apartado virtual "Protección de Datos Personales" de sus portales de internet a partir de los criterios, formatos e indicadores que se detallan en el presente documento.

[2]Toda vez que, con fundamento en la normatividad en la materia, los criterios de la variable "Oficial de Protección de Datos Personales" no son de carácter obligatorio; estos no serán contabilizados ni promediados para la obtención de los índices respectivos, precisando que, tanto su revisión como los medios de verificación que se requieren son únicamente de tipo informativo ya sea para el Instituto, o bien, para las personas titulares de los datos personales; motivo por el cual no forman parte del total que aquí se indica.



Las etapas de evaluación (diagnóstica y vinculante) de acuerdo con la metodología empleada serán las siguientes:

Evaluación diagnóstica:

I. Previo a la evaluación;

II. Evaluación del desempeño de tipo diagnóstico;

III. Integración de resultados;

IV. Elaboración de recomendaciones de carácter general;

V. Elaboración de Informe anual, y

VI. Turno y desahogo de asesorías técnicas (programadas y/o solicitadas).

Evaluación vinculante:

I. Previo a la evaluación;

II. Evaluación del desempeño vinculante;

III. Integración de resultados;

IV. Elaboración de recomendaciones de carácter particular;

V. Seguimiento a recomendaciones de carácter particular;

VI. Elaboración y notificación de dictámenes;

VII. Elaboración de Informe anual, y

VIII. Turno y desahogo de asesorías técnicas (programadas y/o solicitadas).

A) De las vertientes, variables, formatos y criterios

Las vertientes hacen referencia a los principios, deberes y obligaciones con los que deben cumplir los sujetos obligados, a partir de lo establecido en la Ley General, y demás disposiciones que resulten aplicables en la materia. Las vertientes son:

- Principios;
- Deberes;
- Ejercicio de los derechos ARCO;
- Portabilidad;
- Acciones preventivas en materia de protección de datos personales, y
- Responsables en materia de protección de datos personales.

Por su parte, las variables se refieren a diversos aspectos de los principios, deberes u obligaciones identificados en cada una de las vertientes y de ellas se derivan los criterios incluidos en los formatos. A su vez, los criterios se refieren a cada dato o rubro de información que los responsables deberán organizar, actualizar, validar y remitir, dentro de los formatos que se publicarán en el apartado virtual "Protección de Datos Personales".

Las vertientes, variables y formatos, así como el número de criterios que los integran; son los siguientes:

	Formatos		**No. de criterios a cumplir**
Apartado "Protección de datos personales"	Apartado virtual "Protección de datos personales"		4
Vertientes	**Variables**	**Formatos**	**No. de criterios a cumplir**
1.Principios	1.1 Aviso de privacidad integral	1.1 Aviso de privacidad integral	1
	1.2 Mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones de la	1.2 Mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones de la Ley	5

	Ley General y demás disposiciones aplicables	General y demás disposiciones aplicables	
2.Deberes	2.1 Deber de seguridad	2.1 Deber de seguridad	2
	2.2 Deber de confidencialidad y comunicaciones de datos personales	2.2 Deber de confidencialidad y comunicaciones de datos personales	4
3.Ejercicio de los derechos ARCO	3.1 Mecanismos para el ejercicio de los derechos ARCO	3.1 Mecanismos para el ejercicio de los derechos ARCO	5
4.Portabilidad	4.1 Portabilidad de datos personales	4.1 Portabilidad de datos personales	6
5. Acciones preventivas en materia de protección de datos personales	5.1 Evaluación de impacto en la protección de datos personales	5.1 Evaluación de impacto en la protección de datos personales	4
6.Responsables en materia de protección de datos personales	6.1 El Comité de Transparencia y Unidad de Transparencia	6.1 El Comité de Transparencia y Unidad de Transparencia	10
	6.2 Oficial de Protección de Datos Personales	6.2 Oficial de Protección de Datos Personales	2[3]
Total:			41

Los formatos establecidos en el presente documento son de carácter obligatorio en virtud de que, en los mismos se establece de manera sistemática, regulada y ordenada cada uno de los criterios que debe cumplir el responsable, por lo que, estarán disponibles dentro del apartado virtual "Protección de Datos Personales" sección "Herramientas para la evaluación del desempeño" del portal de internet del INAI.

Por su parte, los responsables deberán descargar los formatos del portal de internet del INAI para actualizar y publicar la información generada y organizada de acuerdo con lo establecido en el presente documento. Los formatos no podrán ser modificados al momento de publicar la información.

Capítulo II. Criterios y formatos

[3] Toda vez que, con fundamento en la normatividad en la materia y de acuerdo con lo señalado en la variable correspondiente, estos criterios no son de carácter obligatorio; no serán contabilizados ni promediados para la obtención de los índices correspondientes y, tanto su revisión como los medios de verificación que se requieren son únicamente de tipo informativo ya sea para el Instituto, o bien, para las personas titulares de los datos personales.

Apartado virtual "Protección de datos personales"

En cumplimiento a lo dispuesto en el artículo 250 de los Lineamientos Generales, los responsables deberán contar en su portal de Internet con un apartado denominado "Protección de datos personales", el cual debe contar cuando menos, con el o los avisos de privacidad integrales aplicables a todos los tratamientos de datos personales que el sujeto obligado realiza en ejercicio de sus funciones; los datos de contacto de la Unidad de Transparencia, así como del Oficial de Protección de Datos Personales en caso de haberlo nombrado; y, aquélla información relevante en materia de protección de datos personales que se establece en el presente instrumento técnico de conformidad con el cuarto párrafo del artículo en comento.

Por lo anterior, el apartado virtual "Protección de Datos Personales" contendrá las tres secciones que a continuación se establecen, en el orden y con las denominaciones que se indican:

1. Avisos de privacidad integrales;
2. Datos de contacto de la Unidad de Transparencia y, en su caso, del Oficial de Protección de Datos Personales, y
3. Información relevante en materia de protección de datos personales.

La habilitación del apartado en comento servirá a los responsables como medio para acreditar el cumplimiento de sus obligaciones en materia de protección de datos personales y, por otra parte, será el medio idóneo para que rindan cuentas tanto a los titulares de los datos personales como al Instituto sobre el tratamiento de los datos personales en su posesión.

Asimismo, dicho apartado permitirá que el INAI en su calidad de organismo garante del derecho a la protección de datos personales evalúe el cumplimiento de los principios, deberes y obligaciones en la materia por parte de los sujetos obligados, atendiendo a la obligatoriedad que a estos les corresponde.

Por otra parte, el apartado virtual constituye el repositorio de los medios de verificación documentales que se corroborarán en los ejercicios de evaluación del desempeño, de acuerdo con las características y contenidos establecidos en el presente instrumento técnico.

Finalmente cabe precisar que, al ser el apartado virtual "Protección de Datos Personales" el repositorio de los medios de verificación a evaluar, la ausencia de éste, así como la falta de cumplimiento a las características, orden y contenido establecidos en el presente instrumento, implicará para el Instituto la imposibilidad de llevar a cabo el ejercicio de evaluación del desempeño que corresponda y, en consecuencia, la determinación de incumplimiento de la totalidad de criterios por parte del sujeto obligado que corresponda.

El apartado virtual “Protección de Datos Personales” y la información en él contenida deberán estar disponibles de forma permanente y actualizarse conforme lo determina el presente instrumento técnico.

Para el caso de aquellos sujetos obligados que, por su naturaleza, no cuenten con portal de Internet, deberán habilitar el apartado virtual “Protección de Datos Personales”, así como acreditar el cumplimiento de los principios, deberes y obligaciones que les corresponden en la materia, a través del portal de Internet y de la información y medios de verificación proporcionados por el sujeto obligado responsable o coordinador del sector al que pertenecen.

Criterios:

Apartado virtual “Protección de datos personales”

No.	Criterio	Medio de verificación	
1.	Hipervínculo al apartado denominado “Protección de Datos Personales” publicado en el portal de internet del sujeto obligado en su página de inicio.		
2.	Hipervínculo a la sección “1. Avisos de privacidad integrales” publicada dentro del apartado “Protección de Datos Personales”		
3.	Hipervínculo a la sección “2. Datos de contacto de la Unidad de Transparencia y, en su caso, del Oficial de Protección de Datos Personales[4]” publicada dentro del apartado “Protección de Datos Personales”		
4.	Hipervínculo a la sección “3. Información relevante en materia de protección de datos personales” publicada dentro del apartado “Protección de Datos Personales”		

Vertiente 1: Principios

Variable 1.1: Aviso de privacidad integral

El Aviso de privacidad, con base en la Ley General[5], es el documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de estos.

[4] Toda vez que, con fundamento en la normatividad en la materia, la figura del oficial de protección de datos personales no es de carácter obligatorio; el medio de verificación correspondiente al oficial de protección de datos personales no será contabilizado ni promediado para la obtención de los índices correspondientes, por lo tanto su revisión, en el medio de verificación que se requiere en el presente formato, es de tipo informativo censal para el instituto, e informativo para las personas titulares de los datos personales.

[5] Artículo 3, fracción II de la Ley General.

Por lo anterior, es indispensable que todos los responsables generen el o los avisos de privacidad que correspondan, de acuerdo con las actividades y/o servicios con los que cuenten, y que a su vez impliquen el tratamiento de datos personales.

Estos avisos de privacidad deberán ser puestos a disposición del titular; y en ellos se deberá informar de manera clara y sencilla, las características principales del tratamiento al que serán sometidos sus datos personales, con la finalidad de que el titular, pueda, en su caso, tomar decisiones informadas al respecto.

Por lo anterior, de acuerdo con lo preceptuado en los Lineamientos Generales[6], en el aviso de privacidad queda prohibido lo siguiente:

- Usar frases inexactas, ambiguas o vagas;
- Incluir textos o formatos que induzcan a los titulares a elegir una opción en específico;
- Marcar previamente casillas, en caso de que estas se incluyan, para que los titulares otorguen su consentimiento, o bien, incluir declaraciones orientadas a afirmar que el titular ha consentido el tratamiento de sus datos personales sin manifestación alguna de su parte, y
- Remitir a textos o documentos que no estén disponibles para los titulares.

Las modalidades mediante las cuales se deberá poner a disposición del titular el aviso de privacidad son:

- Simplificado
- Integral

Respecto del aviso de privacidad simplificado, el responsable deberá sujetarse a lo que indiquen los Lineamientos Generales respecto de las finalidades del tratamiento[7], así como en la normatividad que le sea aplicable. Se deberán describir puntualmente y de manera clara, cada una de las finalidades para las cuales se tratarán los datos personales sin que éstas sean inexactas, ambiguas o vagas y se deben distinguir aquellas finalidades que requieren consentimiento del titular.

Además, en caso de tratarse de transferencias, se deberán precisar los destinatarios ya sean nacionales o internacionales, públicos o privados[8].

[6] Artículo 28 de los Lineamientos Generales.
[7] Artículo 31 de los Lineamientos Generales.
[8] Artículo 32 de los Lineamientos Generales.

Asimismo, el responsable deberá difundir los mecanismos y medios con los que cuentan los titulares para manifestar la negativa en el aviso de privacidad; estos mecanismos y medios deberán sujetarse a lo que indiquen la Ley General, los Lineamientos Generales[9] y demás disposiciones que resulten aplicables en la materia.

De igual forma, el responsable está obligado a documentar la puesta a disposición del aviso de privacidad[10].

Los avisos de privacidad deberán ser difundidos en un lugar visible que facilite su consulta y que permita a los responsables acreditar fehacientemente el cumplimiento de esta obligación ante el INAI; en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su comunicación.

Cuando el responsable considere que resulta imposible dar a conocer al titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, se podrán instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios[11], que, en su caso, emita el SNT.

Para dar cumplimiento a esta obligación, los responsables deberán difundir tanto los avisos de privacidad simplificados como los integrales, es decir, por cada actividad y/o servicio en el cual se lleva a cabo el tratamiento de datos personales, se deberán generar ambos avisos.

Los avisos de privacidad simplificados[12] deberán contar con la siguiente información:

- Denominación del responsable;
- Finalidad del tratamiento para el cual se obtienen los datos, distinguiendo aquellas que requieran el consentimiento del titular;
- En caso de realizar transferencias: las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales;
- Las finalidades en caso de realizar transferencias;
- Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular, y
- El sitio donde se podrá consultar el aviso de privacidad integral.

[9] Artículo 33 de los Lineamientos Generales.
[10] Artículo 15 de los Lineamientos Generales.
[11] Artículo 26, cuarto párrafo de la Ley General.
[12] Artículo 27 de la Ley General.

Además de lo anterior, los avisos de privacidad integrales deberán contener al menos lo siguiente[13]:

- El domicilio del responsable;
- Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;
- El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;
- Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular;
- Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
- El domicilio de la Unidad de Transparencia, y
- Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

La carga de la prueba para acreditar la puesta a disposición del aviso de privacidad recaerá, en todos los casos, en el responsable[14].

La información publicada en la presente variable deberá guardar congruencia con lo publicado en las variables Mecanismos para el ejercicio de los derechos ARCO y Transferencias de datos personales.

La información publicada en este apartado deberá cumplir con las *reglas generales de evaluación* establecidas en el presente documento.

Periodo de actualización: Cada vez que exista una modificación, los responsables tendrán hasta 10 días hábiles para actualizar la información.

Conservación: Se debe conservar la información vigente.

Ubicación en el sitio de internet del responsable: De conformidad con lo dispuesto en el artículo 250 de los Lineamientos Generales, la información relativa a la presente variable, así como los medios de verificación correspondientes a cada criterio de evaluación, deberán publicarse en el apartado virtual "Protección de Datos Personales" del portal de internet del sujeto obligado, específicamente en la sección denominada "Avisos de privacidad integrales".

Criterios:

[13] Artículo 28 de la Ley General.
[14] Artículos 45 y 54 de los Lineamientos Generales.

Respecto de las actividades y/o servicios para los cuales se lleva a cabo el tratamiento de datos personales, por ejemplo, para acceder a un trámite, servicio, entre otros, se deberá indicar:

Formato 1.1 Aviso de Privacidad Integral

Ejercicio (año) del que se presenta la información		(AAAA)
Fecha de publicación de la información		(DD/MM/AAAA)
Fecha de la última actualización		(DD/MM/AAAA)
No.	**Criterio**	**Medio de verificación**
1.	Hipervínculo al documento que contenga la información relativa al aviso o avisos de privacidad integrales[15]: a) Denominación del tratamiento de datos personales que lleva a cabo el sujeto obligado (incluido el tratamiento de datos de su personal) b) Tipo de medio por el cual se difunde el aviso de privacidad (Físico / Electrónico / Físico y Electrónico / Óptico / Sonoro / Visual / Otra tecnología)) c) Lugar físico en el cual el titular podrá revisar el aviso de privacidad d) Hipervínculo al aviso de privacidad publicado en el portal de internet del responsable	

Vertiente 1: Principios

Variable 1.2: Mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones de la Ley General y demás disposiciones aplicables.

La Ley General, establece que, para cumplir con el principio de responsabilidad, los sujetos obligados deben implementar los mecanismos previstos en el artículo 30 de esta, los cuales consisten en:

- Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;

[15] Anexo–Guía 1. Información sobre el aviso o los avisos de privacidad integrales.

- Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;
- Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;
- Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;
- Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;
- Establecer procedimientos para recibir y responder dudas y quejas de los titulares;
- Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la Ley General y las demás que resulten aplicables en la materia, y
- Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la Ley General y demás disposiciones que resulten aplicables en la materia.

Lo anterior, con el fin de acreditar el cumplimiento de los principios, deberes y obligaciones[16] establecidos en la Ley General y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y al INAI, caso en el cual deberá observar la Constitución y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines; también[17] resulta aplicable, cuando los datos personales sean tratados por parte de un encargado a solicitud del responsable y al momento de hacer transferencias nacionales o internacionales.

Respecto de los **programas y políticas de protección de datos personales**, con base en los establecido en los Lineamientos Generales[18], los responsables deberán elaborarlos e implementarlos,

[16] Artículo 29 de la Ley General.
[17] Artículo 46, cuarto párrafo de los Lineamientos Generales.
[18] Artículo 47, primer párrafo de los Lineamientos Generales.

y estos documentos tendrán por objeto establecer los elementos y actividades de dirección, operación y control de todos los procesos que, en ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continua. Asimismo, estos documentos deben ser aprobados, coordinados y supervisados por el respectivo Comité de Transparencia[19] y se deberán prever y autorizar recursos[20], de conformidad con la normatividad que resulte aplicable para la implementación y cumplimiento de dichos documentos.

En cuanto al **programa de protección de datos personales** se sugiere que se elabore considerando por lo menos los siguientes puntos[21].

- Objetivos del Programa definidos;
- Responsabilidades dentro del Programa definidas;
- El alcance del Programa;
- El desarrollo de la Política de Gestión de los Datos Personales, en el que se incluya el establecimiento de las obligaciones relevantes en la etapa de obtención, uso y eliminación de los datos personales;
- La definición de revisiones y auditorías a realizar;
- La definición de acciones para la mejora continua del programa, y
- Las sanciones aplicables

Además, por regla general el responsable deberá contar con los **sistemas de supervisión y vigilancia internas y/o externas incluyendo auditorías,** que le permitan revisar periódicamente las políticas y programas que le son aplicables. Estos sistemas deberán estar especificados en el respectivo Programa de protección de datos personales y deberán revisarse al menos cada dos años[22], a menos que el tratamiento de datos personales que lleva a cabo tenga modificaciones sustanciales y que por lo tanto se requiera una actualización previa.

Respecto del **programa de capacitación** que el responsable realice, se deberá atender a lo establecido en el artículo 48 de los Lineamientos Generales.

Con relación al **procedimiento para la atención de dudas y quejas de los titulares**, los responsables deberán establecer y habilitar las acciones o procedimientos que se realizarán para

[19] Artículo 47, segundo párrafo de los Lineamientos Generales.
[20] Artículo 47, tercer párrafo de los Lineamientos Generales.
[21] De acuerdo con el *Documento orientador para la elaboración del Programa de Protección de Datos Personales*, publicado por el INAI como herramienta de facilitación y orientación para los sujetos obligados.
[22] Artículo 49 de los Lineamientos Generales.

recibir y responder estas dudas y quejas de manera que sea de fácil acceso y con la mayor cobertura posible, atendiendo así a lo previsto en los Lineamientos Generales[23].

Las políticas públicas, programas, servicios, sistemas o plataformas que impliquen tratamientos de datos personales; deberán cumplir por diseño[24] y por defecto[25] con las disposiciones previstas en la Ley General y demás que resulten aplicables en la materia.

Para dar cumplimiento a esta obligación, los responsables deberán difundir la información y documentos siguientes:

- Programa de Protección de Datos Personales;
- Políticas de Protección de Datos Personales;
- Programa de Capacitación de Protección de Datos Personales;
- Sistemas de supervisión y vigilancia, y
- Procedimiento de atención de dudas y quejas.

La carga de la prueba para acreditar el cumplimiento de principios, deberes y obligaciones de la Ley General de Datos y demás normatividad aplicable, en todo momento, recaerá en el responsable[26].

La información publicada en el apartado "Programa de capacitación" deberá guardar congruencia con lo publicado en la variable El Comité de Transparencia y Unidad de Transparencia.

La información publicada en este apartado deberá cumplir con las *reglas generales de evaluación* establecidas en el presente documento.

Periodo de actualización:

Programas y políticas de protección de datos personales: Cada vez que exista una modificación sin importar la razón de esta, los responsables tendrán hasta 10 días hábiles para actualizar la información.

Sistemas de supervisión y vigilancia internas y/o externas: éstos deberán actualizarse cada dos años y los responsables tendrán hasta 10 días hábiles para actualizar la información.

Procedimiento para la atención de dudas y quejas de los titulares: Cada vez que exista una modificación, los responsables tendrán hasta 10 días hábiles para actualizar la información.

Conservación: Se debe conservar la información vigente.

---

[23] Artículo 50 de los Lineamientos Generales.
[24] Artículo 51 de los Lineamientos Generales.
[25] Artículo 30, fracción VIII de la Ley General y 52 de los Lineamientos Generales.
[26] Artículos 16, 45, 54, 72, 107 y 118 de los Lineamientos Generales.

Ubicación en el sitio de internet del responsable: De conformidad con lo dispuesto en el artículo 250 de los Lineamientos Generales, la información relativa a la presente variable, así como los medios de verificación correspondientes a cada criterio de evaluación, deberán publicarse en el apartado "Protección de Datos Personales" del portal de internet del sujeto obligado, específicamente en la sección denominada "Información relevante en materia de protección de datos personales".

Criterios:

Formato 1.2. Mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones de la Ley General y demás disposiciones aplicables

Ejercicio (año) del que se presenta la información		(AAAA)
Fecha de publicación de la información		(DD/MM/AAAA)
Fecha de la última actualización		(DD/MM/AAAA)
No.	**Criterio**	**Medio de verificación**
1.	Oficio o instrumento a través del cual se autoriza el destino de recursos para la instrumentación de programas y políticas de protección de datos personales	
2.	Hipervínculo al programa o política de protección de datos personales	
3.	Hipervínculo al programa de capacitación de protección de datos personales	
4.	Hipervínculo al documento en el cual se especifiquen los sistemas de supervisión y vigilancia	
5.	Hipervínculo al documento en el cual el responsable establece el procedimiento para la recepción y respuesta de dudas, y quejas de los titulares en materia de protección de datos personales	

Vertiente 2: Deberes

Variable 2.1: Deber de seguridad

Para el cumplimiento del deber de seguridad el responsable deberá observar lo dispuesto en los artículos 3 fracciones XIV, XX, XXI, XXII y XXIII; 31 a 41 de la Ley General y 55 a 70 de los Lineamientos Generales.

El deber de seguridad deberá observarse durante todo el ciclo de vida de los datos personales, es decir, desde su obtención hasta su eliminación.

Al respecto, todos los responsables deberán:

- Elaborar un documento de seguridad, que describa y dé cuenta de las medidas de seguridad que adopta[27];
- Realizar diversas actividades interrelacionadas para establecer y mantener medidas de seguridad[28];
- Documentar las acciones relativas a las medidas de seguridad en un sistema de gestión[29], y
- En caso de que ocurra alguna vulneración, observar lo establecido en la Ley General y demás disposiciones aplicables en la materia[30].

Documento de seguridad y medidas de seguridad

La implementación de las medidas administrativas, físicas y técnicas contribuye al cumplimiento del deber de seguridad a que se refieren la Ley General y los Lineamientos Generales[31], por parte de los responsables.

Las medidas de seguridad, de conformidad con la Ley General[32], son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales.

Asimismo, cada una de las medidas de seguridad, ya sean administrativas, físicas o técnicas, cuentan con diversas particularidades que contribuyen a proteger los datos personales en posesión de los responsables, contra daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado, así como para garantizar su confidencialidad, integridad y disponibilidad.

Las medidas de seguridad que adopte el responsable deberán considerar[33]:

- El riesgo inherente a los datos personales tratados;
- La sensibilidad de los datos personales tratados;
- El desarrollo tecnológico;
- Las posibles consecuencias de una vulneración para los titulares;
- Las transferencias de datos personales que se realicen;

[27] Artículos 3 fracciones XIV y XX a XXIII; 31 a 36 de la Ley General y 55 de los Lineamientos Generales.
[28] Artículos 33 y 34 de la Ley General y 55 a 64 de los Lineamientos Generales.
[29] Artículo 34 de la Ley General y 65 de los Lineamientos Generales.
[30] Artículos 37 a 41 de Ley General y 66 a 69 de los Lineamientos Generales.
[31] Artículos 31, 32, 33, 34, 35 y 36 de la Ley General y 55 al 65 de los Lineamientos Generales.
[32] Artículo 3, fracción XX, de la Ley General.
[33] Artículo 32 de la Ley General.

- El número de titulares;
- Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
- 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.

Las medidas de seguridad administrativas[34] se refieren a las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Las medidas de seguridad físicas[35] son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Por su parte, las medidas de seguridad técnicas[36] abarcan el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
- Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

[34] Artículo 3, fracción XXI de la Ley General.
[35] Artículo 3, fracción XXII, de la Ley General.
[36] Artículo 3, fracción XXIII, de la Ley General.

- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

El responsable deberá realizar una revisión del marco normativo que regula el tratamiento específico de datos personales, con la finalidad de identificar medidas de seguridad adicionales y analizar la procedencia de su implementación. Como parte de este ejercicio, los responsables deberán tomar en cuenta otras disposiciones vigentes identificadas en materia de seguridad de la información emitidas por otras autoridades, cuando éstas contemplen una mayor protección para el titular o complementen lo dispuesto por la Ley General y demás normatividad aplicable en la materia; lo anterior, considerando que las medidas de seguridad de carácter administrativo, físico y técnico, se consideran mínimos exigibles, por lo que, cada responsable podrá adoptar las medidas adicionales que considere necesarias con la finalidad de brindar mayores garantías para la protección de los datos personales a los que da tratamiento.

Todas las medidas de seguridad antes enunciadas deberán estar descritas de manera general en el documento de seguridad de cada responsable.

El documento de seguridad, de conformidad con la Ley General[37], es el instrumento que describe y da cuenta de manera general de las medidas de seguridad (técnicas, físicas y administrativas) que el responsable ha adoptado con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de los datos personales a los que da tratamiento.

Por lo que, todos los responsables deberán contar un documento de seguridad que, en términos generales, incluya las medidas, controles y acciones necesarias para garantizar la seguridad de los datos personales en su posesión.

Para dar cumplimiento a esta obligación, los responsables deberán elaborar documentos de seguridad que contengan, al menos, lo siguiente[38]:

- El inventario de datos personales y de los sistemas de tratamiento;
- Las funciones y obligaciones de las personas que traten datos personales;
- El análisis de riesgos;
- El análisis de brecha;

[37] Artículo 3, fracción XIV, de la Ley General.
[38] Artículo 35 de la Ley General.

- El plan de trabajo;
- Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
- El programa general de capacitación.

Los puntos antes referidos forman parte de las actividades interrelacionadas para establecer y mantener las medidas de seguridad para la protección de datos personales, las cuales se establecen en el artículo 33 de la Ley General.

Actividades interrelacionadas para establecer y mantener medidas de seguridad

Como parte de las acciones relativas al establecimiento y mantenimiento de medidas de seguridad, las cuales deben estar documentadas y contenidas en el sistema de gestión[39]; el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas[40]:

- Crear **políticas internas para la gestión y tratamiento de los datos personales**, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión[41];
- Definir las **funciones y obligaciones** del personal involucrado en el tratamiento de datos personales[42];
- Elaborar un **inventario de datos personales** y de los sistemas de tratamiento[43];
- Realizar un **análisis de riesgo** de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros[44];
- Realizar un **análisis de brecha**, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable[45];

[39] Artículo 34, primer párrafo, de la Ley General.
[40] Artículo 33 de la Ley General.
[41] Artículo 56 de los Lineamientos Generales.
[42] Artículo 57 de los Lineamientos Generales.
[43] Artículos 58 y 59 de los Lineamientos Generales.
[44] Artículo 60 de los Lineamientos Generales.
[45] Artículo 61 de los Lineamientos Generales.

- Elaborar un **plan de trabajo para la implementación de las medidas de seguridad** faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales[46];
- **Monitorear y revisar de manera periódica las medidas de seguridad** implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales[47], y
- **Diseñar y aplicar diferentes niveles de capacitación** del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales[48].

Sobre las **políticas internas de gestión y tratamiento de datos personales**, los responsables deberán crearlas y considerar para ello, el contexto en el que se llevan a cabo los tratamientos, así como el ciclo de vida de los datos personales, lo que abarca desde el momento en el que se obtienen, el uso que se hace de ellos, hasta que son suprimidos[49].

Los responsables deberán incluir en las políticas internas para la gestión y tratamiento de datos personales, al menos, lo siguiente[50]:

- El cumplimiento de todos los principios, deberes, derechos y demás obligaciones en la materia, de conformidad con lo previsto en la Ley General y demás disposiciones que resulten aplicables en la materia;
- Los roles y responsabilidades específicas de los involucrados internos y externos dentro de su organización, relacionados con los tratamientos de datos personales que se efectúen;
- Las sanciones en caso de incumplimiento;
- La identificación del ciclo de vida de los datos personales respecto de cada tratamiento que se efectúe; considerando la obtención, almacenamiento, uso, procesamiento, divulgación, retención, destrucción o cualquier otra operación realizada durante dicho ciclo en función de las finalidades para las que fueron recabados;

[46] Artículo 62 de los Lineamientos Generales.
[47] Artículo 63 de los Lineamientos Generales.
[48] Artículo 64 de los Lineamientos Generales.
[49] Artículo 33, fracción I de la Ley General.
[50] Artículo 56 de los Lineamientos Generales.

- El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; considerando el análisis de riesgo realizado previamente al tratamiento de los datos personales, y
- El proceso general de atención de los derechos ARCO.

Por otra parte, para **definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales**[51], el responsable tendrá que establecer y documentar sus roles y responsabilidades, así como la cadena de rendición de cuentas, de acuerdo con el sistema de gestión implementado. En este sentido, el responsable deberá llevar a cabo acciones para asegurar que los servidores públicos que están involucrados en el tratamiento de datos personales conozcan sus funciones y las consecuencias de su incumplimiento.

Para llevar a cabo la definición de funciones y obligaciones del personal involucrado en el tratamiento de datos personales, el responsable podrá apoyarse además de la Ley General y demás normatividad aplicable en la materia, en el instrumento que, a nivel interno, desagregue las atribuciones con las que cuenta y las funciones que les corresponde llevar a cabo, como pueden ser de manera enunciativa, más no limitativa, reglamentos internos, estatutos orgánicos, lineamientos, manuales de organización, manuales de funciones, manuales de procedimientos, perfiles de puestos, entre otros.

Por lo que refiere al **inventario de datos personales y de los sistemas de tratamiento,** los responsables deberán elaborarlo a partir de la información básica de cada tratamiento de datos personales que realicen[52].

Para ello, se requiere que al interior de cada responsable se realice un diagnóstico para identificar los tratamientos de datos personales que se llevan a cabo en sus distintas áreas, así como de los sistemas de tratamiento que utilizan. Este diagnóstico consiste en la elaboración de un inventario que contendrá la información básica de cada tratamiento, con la finalidad de contar con un control documentado, preciso y ordenado de los tratamientos realizados.

Este inventario deberá contener, al menos, lo siguiente[53]:

- El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;

[51] Artículo 33, fracción II de la Ley General y artículo 57 de los Lineamientos Generales.
[52] Artículo 33, fracción III de la Ley General y 58 de los Lineamientos Generales.
[53] Artículo 58 de los Lineamientos Generales.

- Las finalidades de cada tratamiento de datos personales;
- El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no;
- El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
- La lista de servidores públicos que tienen acceso a los sistemas de tratamiento;
- En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable, y
- En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.

En la elaboración del inventario, se deberá tener en consideración el ciclo de vida de los datos personales, es decir, su obtención, uso y supresión, de acuerdo con lo que se establece en el artículo 59 de los Lineamientos Generales.

El contar con un inventario de datos personales permitirá identificar los tratamientos que realiza el responsable, así como abonar al cumplimiento del resto de sus obligaciones.

El inventario de los datos personales y de los sistemas de tratamiento formará parte del documento de seguridad de cada responsable[54].

Respecto al **análisis de riesgo,** cabe precisar que, para establecer y mantener las medidas de seguridad, los responsables tendrán que llevar a cabo un análisis de riesgos de los datos personales, donde consideren además de las amenazas y vulnerabilidades existentes, los recursos involucrados en el tratamiento, tales como hardware, software, personal responsable, entre otros[55].

Al realizar el análisis de riesgos, cada responsable deberá considerar lo siguiente[56]:

- Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;

[54] Artículo 35, fracción I de la Ley General.
[55] Artículo 33, fracción IV de la Ley General.
[56] Artículo 60 de los Lineamientos Generales.

- El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida;
- El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
- Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
- Los siguientes factores:[57]
    - El riesgo inherente a los datos personales tratados;
    - La sensibilidad de los datos personales tratados;
    - El desarrollo tecnológico;
    - Las posibles consecuencias de una vulneración para los titulares;
    - Las transferencias de datos personales que se realicen;
    - El número de titulares;
    - Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
    - 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.

El análisis de riesgo tendrá que realizarse de manera previa al tratamiento de los datos personales[58] y deberá estar contenido en el documento de seguridad del responsable[59]. Asimismo, los resultados del análisis de riesgo deberán incluirse en el plan de trabajo de cada responsable[60].

Asimismo, para el establecimiento y mantenimiento de las medidas de seguridad, el responsable deberá realizar un **análisis de brecha**, comparando las medidas de seguridad existentes contra las faltantes dentro de su organización[61].

Derivado de lo anterior, el análisis de brecha a que se refiere la Ley General deberá considerar lo siguiente[62]:

- Las medidas de seguridad existentes y efectivas;
- Las medidas de seguridad faltantes, y

[57] Artículo 32 de la Ley General y artículo 60, fracción V de los Lineamientos Generales.
[58] Artículo 56, fracción V de los Lineamientos Generales.
[59] Artículo 35, fracción III de la Ley General.
[60] Artículo 62 de los Lineamientos Generales.
[61] Artículo 33, fracción V de la Ley General.
[62] Artículo 61 de los Lineamientos Generales.

- La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

El análisis de brecha deberá estar contenido en el documento de seguridad del responsable[63]. De igual forma, los resultados del análisis de brecha deberán incluirse en el plan de trabajo de cada responsable[64].

Por otra parte, dentro de las actividades interrelacionadas para establecer y mantener las medidas de seguridad, el responsable deberá elaborar un **plan de trabajo**[65]. La finalidad de este plan de trabajo será implementar las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.

Es decir, al elaborar el plan de trabajo, el responsable deberá definir lo siguiente[66]:

- Acciones a implementar de acuerdo con el resultado del análisis de riesgos, y
- Acciones a implementar de acuerdo con el análisis de brecha.

Al definir las acciones mencionadas, el responsable deberá priorizar las medidas de seguridad más relevantes e inmediatas a establecer.

Asimismo, al elaborar el plan de trabajo, el responsable deberá considerar lo siguiente[67]:

- Los recursos designados;
- El personal interno y externo en su organización, y
- Las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

De igual forma, el responsable debe considerar que, ante la existencia de vulneraciones de seguridad, tendrá que implementar en su plan de trabajo acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de datos personales si fuese el caso, lo anterior, con la finalidad de que la vulneración ocurrida no se repita.

El plan de trabajo de cada responsable deberá estar contenido en su documento de seguridad[68].

---

[63] Artículo 35, fracción IV de la Ley General.
[64] Artículo 62 de los Lineamientos Generales.
[65] Artículo 33, fracción VI de la Ley General.
[66] Artículo 62, primer párrafo de los Lineamientos Generales.
[67] Artículo 62, segundo párrafo de los Lineamientos Generales.
[68] Artículo 35, fracción V de la Ley General.

De igual forma, como parte del deber de seguridad, los responsables tendrán que **monitorear y revisar de manera periódica las medidas de seguridad que implementan, así como las amenazas y vulneraciones** a las que están sujetos los datos personales tratados[69].

Para llevar a cabo el monitoreo y revisión de las medidas de seguridad, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de datos personales.

La finalidad de las acciones anteriores será verificar el cumplimiento de los objetivos propuestos al interior del responsable y, en su caso, implementar mejoras de manera continua. Por lo anterior, el responsable deberá monitorear continuamente lo siguiente[70]:

- Los nuevos activos que se incluyan en la gestión de riesgos;
- Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
- Las nuevas amenazas que podrían estar activas dentro y fuera de su organización y que no han sido valoradas;
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
- Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
- El cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo, y
- Los incidentes y vulneraciones de seguridad ocurridas.

Asimismo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar tanto la eficacia como la eficiencia de su sistema de gestión.

Los mecanismos establecidos para el monitoreo y revisión de las medidas de seguridad del responsable deberán estar incluidos en su documento de seguridad[71].

[69] Artículo 33, fracción VII de la Ley General.
[70] Artículo 63 de los Lineamientos Generales.
[71] Artículo 35, fracción VI de la Ley General.

Por lo que se refiere a la **capacitación del personal bajo su mando**, el responsable deberá diseñar y aplicar diferentes niveles de capacitación, dependiendo de los roles y responsabilidades de dicho personal, respecto del tratamiento de los datos personales[72].

Para el cumplimiento de esta obligación, el responsable diseñará e implementará programas a corto, mediano y largo plazo con la finalidad de capacitar a los involucrados, tanto internos como externos a su organización.

En el diseño e implementación de los programas de capacitación, el responsable deberá considerar además de los roles y responsabilidades asignadas para el tratamiento y seguridad de los datos personales, el perfil de cada puesto.

Asimismo, el responsable deberá tomar en cuenta lo siguiente[73]:

- Los requerimientos y actualizaciones del sistema de gestión;
- La legislación vigente en materia de protección de datos personales y las mejores prácticas relacionadas con el tratamiento de éstos;
- Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y
- Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Sistema de gestión

Las acciones relativas a las medidas de seguridad para el tratamiento de datos personales deben estar documentadas y contenidas en un sistema de gestión[74].

Por sistema de gestión se entiende, el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad[75] de los datos personales, de conformidad con lo previsto en la Ley General y demás disposiciones aplicables en la materia[76]; tomando asimismo en consideración los estándares nacionales e internacionales de protección de datos personales y seguridad[77].

---

[72] Artículo 33, fracción VIII de la Ley General.
[73] Artículo 64 de los Lineamientos Generales.
[74] Artículo 34, párrafo primero de la Ley General.
[75] Medidas de seguridad de carácter administrativo, físico y técnico; de conformidad con lo dispuesto en el artículo 65 de los Lineamientos Generales.
[76] Artículo 34, párrafo segundo de la Ley General.
[77] Artículo 65 de los Lineamientos Generales.

En la integración e implementación del sistema de gestión, el responsable deberá enfocarse en la protección de los datos personales que posee, contra daño, pérdida, alteración, destrucción o el uso o tratamiento no autorizado, así como en evitar vulneraciones a dichos datos.

El sistema de gestión deberá ser monitoreado y revisado de manera periódica y cada responsable deberá contar con un programa de auditoría, interno y/o externo, que permita verificar su eficacia y eficiencia[78].

Disposiciones en materia de vulneraciones

Con independencia de las demás que señalen las leyes respectivas, se consideran vulneraciones de seguridad, en cualquier fase del tratamiento de datos personales las siguientes [79]:

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

En caso de que exista una vulneración de seguridad que afecte de forma significativa los derechos patrimoniales o morales de los titulares y una vez que ésta ha sido confirmada y que se ha detonado un proceso de revisión exhaustiva al interior para conocer la magnitud de la afectación, el responsable deberá informar dentro de un plazo máximo de setenta y dos horas a[80]:

- El titular, y
- El INAI

Lo anterior, con la finalidad de que los titulares puedan tomar medidas para la defensa de sus derechos.

Se entiende como afectación a los derechos patrimoniales del titular, que la vulneración se relacione, de manera enunciativa más no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular[81].

Como afectación a los derechos morales del titular, se entiende que la vulneración ocurrida se relacione, de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro,

[78] Artículo 63, último párrafo de los Lineamientos Generales.
[79] Artículo 38 de la Ley General.
[80] Artículo 40 de la Ley General y 66 de los Lineamientos Generales.
[81] Artículo 66, tercer párrafo de los Lineamientos Generales.

honor, reputación, vida privada, configuración y aspecto físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste[82].

Al informar al titular sobre estas vulneraciones, el responsable deberá comunicarle, al menos, lo siguiente[83]:

- La naturaleza del incidente o vulneración ocurrida;
- Los datos personales comprometidos;
- Las recomendaciones al titular acerca de las medidas que pueda adoptar para proteger sus intereses;
- Las acciones correctivas realizadas de forma inmediata;
- Los medios donde puede obtener más información al respecto;
- La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente, y
- Cualquier otra información y documentación que considere conveniente para apoyar a los titulares.

El responsable deberá establecer medios específicos para hacer llegar la información antes referida al titular, considerando su perfil, la forma en la que mantienen contacto o comunicación con él, que los medios sean gratuitos, de fácil acceso, con la mayor cobertura posible y que se encuentren habilitados y disponibles en todo momento.

Para notificar al Instituto sobre las vulneraciones ocurridas, el responsable deberá informar por escrito, o bien, a través de cualquier medio habilitado para el efecto, al menos, lo siguiente[84]:

- La hora y fecha de la identificación de la vulneración;
- La hora y fecha del inicio de la investigación sobre la vulneración;
- La naturaleza del incidente o vulneración ocurrida;
- La descripción detallada de las circunstancias en torno a la vulneración ocurrida;
- Las categorías y número aproximado de titulares afectados;
- Los sistemas de tratamiento y datos personales comprometidos;
- Las acciones correctivas realizadas de forma inmediata;
- La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;

[82] Artículo 66, último párrafo de los Lineamientos Generales.
[83] Artículo 41 de la Ley General y artículo 68 de los Lineamientos Generales.
[84] Artículo 40 de la Ley General y artículo 67 de los Lineamientos Generales.

- Las recomendaciones dirigidas al titular;
- El medio puesto a disposición del titular para que pueda obtener más información al respecto;
- El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar más información al Instituto, en caso de requerirse, y
- Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

De igual forma, como resultado de las vulneraciones de seguridad ocurridas, el responsable deberá integrar una bitácora en la que registre la información detallada de las mismas. La bitácora de vulneraciones deberá contener, al menos, lo siguiente[85]:

- Descripción de la vulneración de seguridad ocurrida;
- Fecha en la que ocurrió;
- Motivo de la vulneración de seguridad;
- Acciones correctivas implementadas de forma inmediata, y
- Acciones correctivas implementadas de forma definitiva.

Asimismo, ante una vulneración de seguridad, el responsable tendrá que analizar las causas que la produjeron e implementar en su plan de trabajo, acciones tanto preventivas como correctivas, con la finalidad de adaptar las medidas de seguridad al tratamiento de datos personales que lleva a cabo y con ello evitar que la vulneración ocurrida se repita[86].

Cabe subrayar que, en caso de que exista un encargado, el responsable será corresponsable por las vulneraciones de seguridad que ocurran en el tratamiento de datos personales que lleve a cabo el encargado a nombre y por cuenta de éste[87].

Igualmente, al adoptar y mantener sus medidas de seguridad, cada responsable deberá considerar, entre otros aspectos, las posibles consecuencias de una vulneración para los titulares; las vulneraciones previas ocurridas en sus sistemas de tratamiento[88]; así como el monitoreo y revisión periódica de dichas medidas de seguridad, incluyendo las amenazas y vulneraciones a las que están sujetos los datos personales[89].

---

[85] Artículo 39 de la Ley General.
[86] Artículo 37 de la Ley General.
[87] Artículo 108, segundo párrafo de los Lineamientos Generales.
[88] Artículo 32, fracción IV y VII de la Ley General.
[89] Artículos 33, fracción VII y 36, fracción IV de la Ley General.

Asimismo, una vez que el responsable cuente con un documento de seguridad deberá actualizarlo ante la presentación de diversos supuestos, entre ellos, como consecuencia de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida y resultado de la implementación de acciones correctivas y preventivas ante una vulneración de seguridad[90].

Cabe precisar que, como parte del análisis de riesgos, el responsable deberá considerar las consecuencias negativas que pudieran resultar para los titulares a partir de una vulneración de seguridad ocurrida[91].

La carga de la prueba para acreditar el cumplimiento del deber de seguridad recaerá, en todo momento, en el responsable[92].

Finalmente, y teniendo en consideración la sensibilidad y relevancia de los datos personales a los que da tratamiento cada responsable, así como de todo aspecto relacionado con la seguridad de estos; con el objetivo de evitar la publicación de información clasificada, es indispensable que, en los criterios en los que así se precise, se muestre la versión pública[93] de los documentos solicitados. La publicación de la versión íntegra de los documentos solicitados, sin excepción, será considerada como incumplimiento al presente documento; lo cual no limita las facultades de investigación y verificación del Instituto.

La información publicada en este apartado deberá guardar congruencia con la variable Relación del responsable y encargado.

La información publicada en este apartado deberá cumplir con las *reglas generales* de evaluación establecidas en el presente documento.

Periodo de actualización: Trimestral, o en su caso, cuando ocurra alguna actualización. El responsable tendrá hasta 10 días hábiles para actualizar la información.

Conservación: Se debe conservar la información vigente.

Ubicación en el sitio de internet del responsable: De conformidad con lo dispuesto en el artículo 250 de los Lineamientos Generales, la información relativa a la presente variable, así como los medios de verificación correspondientes a cada criterio de evaluación, deberán publicarse en el apartado

[90] Artículo 36, fracciones III y IV de la Ley General.
[91] Artículo 60, fracción IV de los Lineamientos Generales.
[92] Artículo 72 de los Lineamientos Generales.
[93] Artículo 3, fracción XXI de la Ley General de Transparencia.

"Protección de Datos Personales" del portal de internet del sujeto obligado, específicamente en la sección denominada "Información relevante en materia de protección de datos personales".".

Criterios:

Formato 2.1 Deber de seguridad

Ejercicio (año) del que se presenta la información		(AAAA)
Fecha de publicación de la información		(DD/MM/AAAA)
Fecha de la última actualización		(DD/MM/AAAA)
No.	**Criterio**	**Medio de verificación**
1.	Hipervínculo a la **versión pública** del documento de seguridad del responsable, testando únicamente lo relativo al plan de trabajo que contiene, además, el análisis de riesgo y brecha **Por ningún motivo debe incluirse en este apartado el documento de seguridad integro con el que cuenta el responsable. El documento de seguridad deberá publicarse protegiendo el plan de trabajo, el análisis de riesgo y el análisis de brecha respectivos; lo que implica que en caso de que se dejen visibles, sin excepción, será considerado como incumplimiento al presente criterio**	
2.	Hipervínculo al documento que contiene las políticas internas de gestión y tratamiento de los datos personales	

Vertiente 2: Deberes

Variable 2.2: Deber de confidencialidad y comunicaciones de datos personales

Para el cumplimiento del deber de confidencialidad y comunicaciones de datos personales el responsable deberá observar lo dispuesto en los artículos 22 fracción II, 42, 58, 59, 64, 65, 66, 67, 68, 69, 70 y 71 de la Ley General y 46, 71, 72, 109, 110, 111, 113, 115, 116, 117 y 118 de los Lineamientos Generales.

Con independencia de lo establecido en las disposiciones en materia de acceso a la información pública, con el objeto de proteger los datos personales a los que da tratamiento, el responsable deberá establecer controles dirigidos a asegurar la confidencialidad que deben guardar todas las personas que intervienen en cualquier fase del tratamiento de datos personales. La obligación de confidencialidad debe subsistir aún después de finalizar la relación entre el responsable y el personal[94].

En los casos en los que el responsable cuente con un Encargado[95], deberá formalizar la relación respectiva mediante contrato o cualquier otro documento, en cual se establecerá como cláusula

[94] Artículo 42 de la Ley General.
[95] Artículo 3, fracción XV de la Ley General.

general relacionada con los servicios que este preste, el guardar confidencialidad respecto de los datos personales tratados[96].

En las actividades de tratamiento de datos personales, realizadas por el encargado, este no ostentará poder alguno de decisión sobre el alcance y contenido, de igual forma limitará sus actuaciones a los términos fijados por el responsable[97].

El responsable será corresponsable por las vulneraciones de seguridad ocurridas en el tratamiento de datos personales que efectué el encargado a nombre y por cuenta de este.

La relación entre el responsable y el encargado deberá formalizarse mediante contrato o cualquier otro instrumento jurídico que decida el responsable y que permita acreditar su existencia, alcance y contenido. El instrumento jurídico mediante el cual decida el responsable formalizar la relación de servicios que preste el encargado, deberá prever, al menos las siguientes cláusulas generales[98]:

- Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;
- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
- Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;
- Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;
- Guardar confidencialidad respecto de los datos personales tratados;
- Suprimir y devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
- Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación o por mandato expreso de la autoridad competente.

Para la prestación de los servicios del encargado, además de las cláusulas generales anteriores, el responsable deberá prever en el instrumento jurídico las siguientes obligaciones[99]:

[96] Artículo 59, fracción V de la Ley General.
[97] Artículo 58 de la Ley General.
[98] Artículo 59 de la Ley General.
[99] Artículo 109 de los Lineamientos Generales.

- Permitir al Instituto o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales;
- Colaborar con el Instituto en las investigaciones previas y verificaciones que lleve a cabo en términos de lo dispuesto en la Ley General y demás normatividad aplicable en la materia, proporcionando información y documentación que se estime necesaria para tal efecto, y
- Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.

Los acuerdos entre el responsable y el encargado relacionados con el tratamiento de datos personales no deberán contravenir la Ley General, las disposiciones aplicables, así como lo establecido en el aviso de privacidad que corresponda.

Al momento de realizar transferencias de datos personales nacionales o internaciones, el responsable deberá aplicar el principio de responsabilidad[100].

El encargado también podrá subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del responsable, siempre y cuando medie autorización expresa de este último, como consecuencia el subcontratado asumirá el carácter de encargado conforme a lo establecido en la Ley General y demás disposiciones que resulten aplicables en la materia.

Cuando en el instrumento jurídico mediante el cual se haya formalizado la relación entre el responsable y el encargado, se establezca que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización a la que refiere el párrafo anterior se entenderá como otorgada a través de lo estipulado, siempre y cuando medie la autorización expresa del responsable.

Obtenida la autorización expresa del responsable, el encargado deberá formalizar la relación adquirida con el subcontratado a través de algún instrumento jurídico que decida, el cual permita acreditar la existencia, alcance y contenido de la prestación del servicio en términos de lo previsto en la Ley General.

Para los servicios de subcontratación que impliquen tratamiento de datos personales, el instrumento jurídico que suscriba el encargado con el subcontratado deberá prever, al menos las cláusulas generales y las obligaciones antes descritas[101].

[100] Artículo 46 de los Lineamientos Generales.
[101] Artículo 110 de los Lineamientos Generales.

Asimismo, para el caso en que existan tratamientos de datos personales en los que el responsable se adhiera a servicios, aplicaciones e infraestructura de cómputo en la nube[102] y otras materias, mediante condiciones o cláusulas generales de contratación; exclusivamente podrá utilizar servicios en los que el o los proveedores guarden confidencialidad respecto de los datos personales sobre los que se preste el servicio[103].

Esto es, el responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la Ley General y demás disposiciones que resulten aplicables en la materia.

Los proveedores de servicios de cómputo en la nube y otras materias que impliquen tratamiento de datos personales, para efectos de la Ley General y demás disposiciones aplicables en la materia, tendrán el carácter de encargados[104].

El responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor cumpla, al menos, con lo siguiente[105]:

- Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley General y demás normatividad aplicable en la materia;
- Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
- Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y
- Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

[102] Artículo 3, fracción VI de la Ley General.
[103] Artículo 64, fracción I inciso d) de la Ley General.
[104] Artículo 111 de los Lineamientos Generales.
[105] Artículo 64 de la Ley General.

Cuente con mecanismos, al menos, para:

- Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
- Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
- Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;
- Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, e
- Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

El responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales.

Para el caso que el encargado y subcontratado incumplan las obligaciones contraídas con el responsable y decidan y determinen por si mismos, los fines, medios y demás cuestiones relacionadas con el tratamiento de los datos personales, asumirán el carácter de responsable de conformidad con la normatividad que les resulte aplicable en función de su naturaleza pública o privada[106].

Por otra parte, cuando el responsable realice algún tipo de transferencia[107], el receptor de los datos personales deberá llevar a cabo el tratamiento de datos personales, garantizando su confidencialidad[108].

Toda transferencia de datos personales sea nacional o internacional, se encuentra sujeta al consentimiento de su titular[109]. Por regla general, el consentimiento será tácito, salvo que una ley exija al responsable recabar el consentimiento expreso del titular para la transferencia de sus datos personales[110].

La Ley General, establece excepciones a las transferencias de datos, en las cuales el responsable no estará obligado a recabar el consentimiento del titular.[111]

---

[106] Artículo 112 de los Lineamientos Generales.
[107] Artículo 3, fracción XXXII de la Ley General.
[108] Artículo 67 de la Ley General.
[109] Artículo 65 de la Ley General.
[110] Artículo 113, segundo párrafo de los Lineamientos Generales.
[111] Artículos 22 fracción II y 70 de la Ley General.

Todas las transferencias deberán formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, conforme a la normatividad aplicable al responsable, las cuales permitirán demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes, limitando el tratamiento de los datos personales transferidos a las finalidades que la justifiquen[112].

Al momento de realizar transferencias de datos personales nacionales o internaciones, el responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General y demás disposiciones aplicables en la materia[113].

Los casos de excepción se dan cuando[114]:

- Tratándose de una transferencia nacional y se realice entre responsables, en el cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos;
- Tratándose de una transferencia internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México,
- La transferencia internacional, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y el responsable receptor sean homólogas, o
- Las finalidades que motivan la transferencia internacional sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.

Tanto en las transferencias nacionales como en las internacionales, el responsable, deberá comunicar al receptor de los datos personales el aviso de privacidad, mediante el cual se tratan los datos personales del titular[115].

Tratándose de transferencias nacionales, el receptor de los datos personales asume el carácter de responsable[116], y deberá tratar los datos personales comprometiéndose a garantizar la

[112] Artículo 66 de la Ley General.
[113] Artículo 46 de los Lineamientos Generales.
[114] Artículo 66 de la Ley General, fracciones I y II.
[115] Artículo 69 de la Ley General.
[116] Artículo 115 de los Lineamientos Generales.

confidencialidad y únicamente los utilizará para los fines que fueron transferidos, atendiendo a lo contenido en el aviso de privacidad que le será comunicado por el responsable transferente[117].

Para el caso de transferencias fuera del territorio nacional, el responsable sólo podrá realizarlas cuando el tercero receptor, encargado o destinatario se obligue a proteger los datos personales conforme a los principios, deberes y demás obligaciones similares o equiparables a las establecidas en la Ley General y demás normatividad aplicable en la materia, así como los términos previstos en el aviso de privacidad que le será comunicado por el responsable transferente[118].

El responsable podrá solicitar la opinión del Instituto, respecto de las transferencias internacionales de datos personales que pretendan realizar, conforme a lo establecido en la Ley General y demás normatividad aplicable en la materia, la solicitud deberá describir las generalidades y particularidades de la transferencia internacional de datos personales que se pretende efectuar[119].

Al momento de realizar transferencias de datos personales nacionales o internaciones, el responsable deberá aplicar el principio de responsabilidad[120].

Las transferencias no abarcan las remisiones de datos personales, que son las comunicaciones de datos personales realizadas exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano, las cuales no requieren ser informadas al titular, ni contar con su consentimiento[121]; asimismo, no incluye el intercambio de información entre las unidades administrativas del propio sujeto obligado[122].

Para el caso de remisiones fuera del territorio nacional, el responsable sólo podrá realizarlas cuando el tercero receptor o encargado se obligue a proteger los datos personales conforme a los principios y deberes establecidas en la Ley General y demás disposiciones aplicables en la materia[123].

---

[117] Artículo 67 de la Ley General.
[118] Artículo 68 de la Ley General y artículo 116 de los Lineamientos Generales.
[119] Artículo 117, fracción II de los Lineamientos Generales.
[120] Artículo 46 de los Lineamientos Generales.
[121] Artículo 71 de la Ley General.
[122] Artículo 3 fracción XXVII de la Ley General y Acuerdo mediante el cual se emiten las recomendaciones en materia de acceso a la información y datos personales ante cambios de titulares de Unidad de Transparencia, de Comité de Transparencia y de Servidores Públicos a cargo el tratamiento de datos personales. Apartado 3. Recomendaciones en materia de datos personales, inciso H. Transferencias de datos personales (pág. 20).
[123] Artículo 68 de la Ley General.

La carga de la prueba para acreditar el cumplimiento del deber de confidencialidad recaerá, en todo momento, en el responsable[124]; de igual forma, por lo que se refiere al cumplimiento de las obligaciones relativas a las transferencias de datos personales[125].

La información publicada en este apartado deberá guardar congruencia con las variables, Vulneraciones de seguridad, el Comité de Transparencia y Unidad de Transparencia; del presente documento.

La información publicada en este apartado deberá cumplir con las *reglas generales de evaluación* establecidas en el presente documento.

Periodo de actualización: Trimestral, o en su caso, cuando ocurra alguna actualización. El responsable tendrá hasta 10 días hábiles para actualizar la información.

Conservación: Se debe conservar la información vigente.

Ubicación en el sitio de internet del responsable: De conformidad con lo dispuesto en el artículo 250 de los Lineamientos Generales, la información relativa a la presente variable, así como los medios de verificación correspondientes a cada criterio de evaluación, deberán publicarse en el apartado "Protección de Datos Personales" del portal de internet del sujeto obligado, específicamente en la sección denominada "Información relevante en materia de protección de datos personales".

Criterios:

Formato 2.2 Deber de confidencialidad y comunicaciones de datos personales

Ejercicio (año) del que se presenta la información		(AAAA)
Fecha de publicación de la información		(DD/MM/AAAA)
Fecha de la última actualización		(DD/MM/AAAA)
No.	**Criterio**	**Medio de verificación**
1.	Hipervínculo al documento mediante el cual se establecen los controles dirigidos a asegurar la confidencialidad que deben guardar todas las personas que intervienen en cualquier fase del tratamiento de datos personales. Los controles deben identificarse con claridad de forma sencilla.	

[124] Artículo 72 de los Lineamientos Generales.
[125] Artículo 118 de los Lineamientos Generales.

2.	Hipervínculo al documento que contenga la relación de los instrumentos jurídicos que regulan la relación con los encargados, en cual se establecerá como cláusula general el guardar confidencialidad respecto de los datos personales tratados por el encargado. El documento deberá contener la denominación e hipervínculo de la versión pública de cada instrumento jurídico y su finalidad, así como indicar si estos incluyen la cláusula general de confidencialidad[126] En caso de que no aplique, el responsable deberá especificar que a la fecha no se cuenta con Encargado(s).	
3.	Hipervínculo al documento que contenga la relación de los instrumentos jurídicos mediante los cuales se formaliza la contratación o adhesión a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias, en los cuales se establezcan las condiciones o cláusulas generales de contratación, incluidas aquéllas en las cuales el o los proveedores se obliguen a guardar confidencialidad respecto de los datos personales sobre los que se preste(n) el servicio. El documento deberá contener la denominación e hipervínculo de la versión pública de cada instrumento jurídico, su finalidad e indicar si incluyen las condiciones o cláusulas generales de la contratación, así como la cláusula general de confidencialidad[127] En caso de que no aplique, el responsable deberá especificar que a la fecha no se cuenta con proveedor(es) de servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias.	
4.	Hipervínculo al documento que contenga la relación de los instrumentos jurídicos mediante los cuales se formalizan las transferencias de datos personales, y en los cuales el receptor de los datos personales se obliga a garantizar la confidencialidad de los datos personales a los que da tratamiento. El documento deberá contener la denominación e hipervínculo de la versión pública de cada instrumento jurídico, su finalidad, breve descripción de la forma en la que se obtuvo el consentimiento del titular, o bien, especificar alguna de las excepciones establecidas en los artículos 22 fracción II y/o 70 de la Ley General; medio o forma por el que el responsable comunicó al receptor de los datos personales, el aviso de privacidad conforme al cual se tratan los datos personales frente al titular; así como indicar si estos incluyen la cláusula general de confidencialidad[128] En caso de que no aplique, el responsable deberá especificar que a la fecha no se han realizado transferencias, o bien, que no aplica por actualizarse alguno de los supuestos que establece el artículo 66 fracciones I y II de la Ley General.	

Vertiente 3: Ejercicio de los derechos ARCO

Variable 3.1: Mecanismos para el ejercicio de los derechos ARCO

Los derechos ARCO, de conformidad con la Ley General son los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales[129].

[126] Ver Anexo-Guía 2. Instrumentos jurídicos que regulan la relación con los Encargados con cláusula general de guardar confidencialidad.

[127] Ver Anexo-Guía 3. Instrumentos jurídicos mediante los cuales se formaliza la contratación o adhesión a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias.

[128] Ver Anexo-Guía 4. Transferencias de datos personales.

[129] Artículo 3, fracción XI, de la Ley General.

Estos derechos implican que tanto el titular como en su caso, su representante, puedan solicitar al responsable que trata sus datos personales el acceso, rectificación, cancelación u oposición a dicho tratamiento.

Los titulares conocerán a través del aviso de privacidad que el responsable ponga a su disposición; los mecanismos, medios y procedimientos para el ejercicio de los derechos ARCO.

Derecho de acceso[130]

Todos los titulares tienen derecho a solicitar el acceso a los datos personales que les pertenecen y que se encuentren en bases de datos, sistemas, archivos, expedientes o cualquier tipo de registro de los responsables, así como de conocer información relacionada con el uso que se da a su información personal, es decir, las condiciones y generalidades de su tratamiento.

Al presentar una solicitud de acceso a datos personales, el titular deberá señalar la modalidad en la que prefiere que sus datos se reproduzcan y el responsable deberá atender a dicha modalidad, salvo que exista una imposibilidad física o jurídica, en cuyo caso ofrecerá otras alternativas.

La obligación de acceso a los datos personales se dará por cumplida cuando el responsable – previa acreditación de la identidad del titular y, en su caso, la identidad y personalidad de su representante – ponga a disposición del titular, sus datos personales mediante consulta directa en el sitio donde se encuentren, o mediante la expedición de copias simples, copias certificadas, medios magnéticos, ópticos, sonoros, visuales u holográficos, o cualquier otra tecnología que determine el titular, dentro del plazo de quince días contados a partir del día siguiente en que se hubiere notificado la respuesta al titular[131].

Derecho de rectificación[132]

Los titulares tienen derecho a solicitar al responsable que trata sus datos personales la rectificación o corrección de estos. Lo anterior, será aplicable cuando se identifique que los datos son inexactos, incompletos o no se encuentren actualizados.

La obligación de rectificar los datos personales se dará por cumplida cuando el responsable notifique al titular, una constancia que acredite la corrección solicitada, dentro del plazo de quince días[133].

---

[130] Artículo 44 de la Ley General.
[131] Artículo 92 de los Lineamientos Generales.
[132] Artículo 45 de la Ley General.
[133] Artículo 93 de los Lineamientos Generales.

Derecho de cancelación[134]

El titular tiene derecho a solicitar a los responsables la cancelación de sus datos personales de sus archivos, registros, expedientes y sistemas, con la finalidad de que ya no estén en su posesión y dejen de ser tratados.

Al ejercer este derecho, el titular deberá señalar las causas que lo motivaron a solicitar la supresión de sus datos personales.

La obligación de cancelar los datos personales se dará por cumplida cuando el responsable – previa acreditación de la identidad del titular y, en su caso, la identidad y personalidad de su representante – le notifique una constancia, dentro del plazo de quince días[135], que señale: los documentos, bases de datos personales, archivos, registros, expedientes y/o sistemas de tratamiento donde se encuentren los datos personales objeto de cancelación; el periodo de bloqueo de los datos personales, en su caso; las medidas de seguridad de carácter administrativo, físico y técnico implementadas durante el periodo de bloqueo, en su caso, y las políticas, métodos y técnicas utilizadas para la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima[136].

Derecho de oposición[137]

Los titulares podrán oponerse al tratamiento de sus datos personales por parte del responsable o exigir que se cese en el mismo cuando:

- Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, y
- Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

Al ejercer el derecho de oposición al tratamiento de sus datos personales, el titular deberá señalar las causas legítimas o la situación específica que lo llevó a solicitar el cese, así como el daño o perjuicio

[134] Artículo 46 de la Ley General.
[135] Artículo 94 de los Lineamientos Generales.
[136] Artículo 94 de los Lineamientos Generales.
[137] Artículo 47 de la Ley General.

que le causaría la persistencia del tratamiento o bien, las finalidades por las que requiere ejercer este derecho.

La obligación de cesar el tratamiento de los datos personales se dará por cumplida cuando el responsable notifique al titular, una constancia que señale dicha situación dentro del plazo de quince días[138].

Reglas generales del ejercicio de los derechos ARCO

En el ejercicio de estos derechos, se deberán observar las siguientes reglas de carácter general:

- Debe ser gratuito, salvo las excepciones dispuestas en la Ley General;
- La Unidad de Transparencia de cada responsable, es el área encargada de gestionar las solicitudes para el ejercicio de los derechos ARCO, así como de auxiliar y orientar al titular en la elaboración de las solicitudes para el ejercicio de sus derechos ARCO;
- Se debe acreditar la identidad del titular y, en su caso, la identidad y personalidad de su representante;
- Cuando se trate de menores de edad o personas que se encuentren en estado de interdicción o incapacidad, se deberán observar las reglas de representación dispuestas en las leyes civiles;
- Tratándose de datos concernientes a personas fallecidas, la persona que acredite tener un interés jurídico podrá ejercer los derechos ARCO, siempre que el titular hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial al respecto. En caso de que la persona fallecida no hubiere expresado su voluntad, bastará con que la persona que pretende ejercer los derechos ARCO acredite su interés jurídico en los términos previstos en la Ley General y demás disposiciones que resulten aplicables en la materia;
- Los responsables deben contar con medios y procedimientos sencillos y de fácil acceso, con la mayor cobertura posible para el ejercicio de los derechos ARCO;
- En el diseño e implementación de las políticas internas para la gestión y tratamiento de los datos personales, cada responsable debe incluir, entre otros, el proceso general de atención de los derechos ARCO;

[138] Artículo 95 de los Lineamientos Generales.

- El plazo de respuesta no debe exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud;
- Las solicitudes para el ejercicio de los derechos ARCO se presentarán ante la Unidad de Transparencia del responsable que el titular considere competente;
- Las solicitudes para el ejercicio de los derechos ARCO se podrán realizar mediante escrito libre, formatos, medios electrónicos o cualquier otro que establezca el Instituto;
- El responsable debe dar trámite a todas las solicitudes para el ejercicio de los derechos ARCO y entregar el acuse de recibo correspondiente;
- Los responsables no podrán imponer mayores requisitos que los establecidos por la Ley General;
- Contra la negativa de dar trámite a una solicitud para el ejercicio de los derechos ARCO o ante la falta de respuesta del responsable, procede el recurso de revisión a que se refiere el artículo 94 de la Ley General, y
- El ejercicio de cualquiera de los derechos ARCO no constituye un requisito previo, ni impide el ejercicio de otro.

En la solicitud para el ejercicio de los derechos ARCO, se deberá incluir[139]:

- El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;
- Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;
- De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;
- La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los citados derechos, salvo que se trate del derecho de acceso;
- La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y
- Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.

[139] Artículo 52 de la Ley General.

Cuando alguna solicitud no cumpla con los requisitos antes señalados y el responsable no cuente con elementos para subsanarla, se debe prevenir al titular para que subsane las omisiones identificadas dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO, por una sola ocasión, para que subsane dentro de un plazo de diez días contados a partir del día siguiente al de la notificación[140].

La carga de la prueba para acreditar el cumplimiento de las obligaciones relacionadas con los mecanismos para el ejercicio de los derechos ARCO, recaerá, en todo momento, en el responsable[141].

La información publicada en este apartado deberá cumplir con las *reglas generales de evaluación* establecidas en el presente documento.

La información publicada en la presente variable deberá guardar congruencia con lo publicado en las variables, Aviso de privacidad, Actividades interrelacionadas para establecer y mantener las medidas de seguridad y Transferencias y Remisiones de datos personales, del presente documento.

Periodo de actualización: Trimestral. El responsable tendrá hasta 10 días hábiles para actualizar la información.

Conservación: Se debe conservar la información vigente.

Ubicación en el sitio de internet del responsable: De conformidad con lo dispuesto en el artículo 250 de los Lineamientos Generales, la información relativa a la presente variable, así como los medios de verificación correspondientes a cada criterio de evaluación, deberán publicarse en el apartado "Protección de Datos Personales" del portal de internet del sujeto obligado, específicamente en la sección denominada "Información relevante en materia de protección de datos personales".

Criterios:

Formato 3.1 Mecanismos para el ejercicio de los derechos ARCO

Ejercicio (año) del que se presenta la información		(AAAA)
Fecha de publicación de la información		(DD/MM/AAAA)
Fecha de la última actualización		(DD/MM/AAAA)
No.	**Criterio**	**Medio de verificación**

[140] Artículo 87 de los Lineamientos Generales.
[141] Artículo 107 de los Lineamientos Generales.

1.	Hipervínculo del documento que contiene los medios y procedimientos habilitados por el responsable para atender las solicitudes para el ejercicio de los derechos ARCO	
2.	Hipervínculo al documento que detalla la siguiente información relativa a las solicitudes para el ejercicio del derecho de Acceso a datos personales recibidas por el sujeto obligado[142]: a) Número de solicitudes recibidas b) Número de solicitudes atendidas dentro del plazo legal establecido c) Número de solicitudes que no se atendieron dentro del plazo legal establecido En caso de no haber recibidos solicitudes para el ejercicio del derecho de Acceso a datos personales, deberá especificarlo en el presente formato sin que sea necesario publicar documento alguno.	
3.	Hipervínculo al documento que detalla la siguiente información relativa a las solicitudes para el ejercicio del derecho de Rectificación de datos personales recibidas por el sujeto obligado[143]: a) Número de solicitudes recibidas b) Número de solicitudes atendidas dentro del plazo legal establecido c) Número de solicitudes que no se atendieron dentro del plazo legal establecido En caso de no haber recibido solicitudes para el ejercicio del derecho de Rectificación de datos personales, deberá especificarlo en el presente formato sin que sea necesario publicar documento alguno.	
4.	Hipervínculo al documento que detalla la siguiente información relativa a las solicitudes para el ejercicio del derecho de Cancelación de datos personales recibidas por el sujeto obligado[144]: a) Número de solicitudes recibidas b) Número de solicitudes atendidas dentro del plazo legal establecido c) Número de solicitudes que no se atendieron dentro del plazo legal establecido En caso de no haber recibido solicitudes para el ejercicio del derecho de Cancelación de datos personales, deberá especificarlo en el presente formato sin que sea necesario publicar documento alguno.	
5.	Hipervínculo al documento que detalla la siguiente información relativa a las solicitudes para el ejercicio del derecho de Oposición al tratamiento de datos personales recibidas por el sujeto obligado[145]: a) Número de solicitudes recibidas b) Número de solicitudes atendidas dentro del plazo legal establecido c) Número de solicitudes que no se atendieron dentro del plazo legal establecido En caso de no haber recibidos solicitudes para el ejercicio del derecho de Oposición al tratamiento de datos personales, deberá especificarlo en el presente formato sin que sea necesario publicar documento alguno.	

[142] Ver Anexo-Guía 5. Información sobre derechos ARCO.
[143] Ver Anexo-Guía 5. Información sobre derechos ARCO.
[144] Ver Anexo-Guía 5. Información sobre derechos ARCO.
[145] Ver Anexo-Guía 5. Información sobre derechos ARCO.

Vertiente 4: Portabilidad

Variable 4.1: Portabilidad de datos personales

La portabilidad de datos personales tiene por objeto que el titular solicite[146]:

- Una copia de los datos personales que hubiere facilitado directamente al responsable, en un formato estructurado y comúnmente utilizado, que le permita seguir utilizándolos y, en su caso, entregarlos a otro responsable para su reutilización y aprovechamiento en un nuevo tratamiento, sin que lo impida el responsable al que el titular hubiere facilitado los datos personales, y
- La transmisión de sus datos personales a un responsable receptor, siempre y cuando sea técnicamente posible, el titular hubiere facilitado directamente sus datos personales al responsable transmisor y el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.

Al respecto, la Ley General establece que cuando los responsables traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, deben dar copia de los datos objeto del tratamiento a los titulares en un formato que les permita seguir utilizándolos, incluyendo el mayor número de metadatos[147] que se hayan generado y obtenido[148].

De acuerdo con los Lineamientos de Portabilidad, se entiende que un formato estructurado y comúnmente utilizado, deberá cumplir con lo siguiente[149]:

- Que se trate de un formato electrónico accesible y legible por medios automatizados, de tal forma que éstos puedan identificar, reconocer, extraer, explotar o realizar cualquier otra operación con datos personales específicos;
- El formato permita la reutilización y/o aprovechamiento de los datos personales, y
- El formato sea interoperable con otros sistemas informáticos.

Con base en los Lineamientos de Portabilidad, se procederá a ésta sólo si se actualizan las siguientes condiciones[150]:

- El tratamiento se efectúe por medios automatizados o electrónicos y en un formato estructurado y comúnmente utilizado;

[146] Artículo 7 de los Lineamientos de Portabilidad.
[147] Artículo 18 de los Lineamientos de Portabilidad.
[148] Artículo 57, primer párrafo de la Ley General.
[149]Artículo 6, fracciones I a la III de los Lineamientos de Portabilidad.
[150] Artículo 8 de los Lineamientos de Portabilidad.

- Los datos personales del titular se encuentren en posesión del responsable o sus encargados;
- Los datos personales conciernan al titular, o bien, a personas físicas vinculadas a un fallecido que tengan un interés jurídico;
- El titular hubiere proporcionado directamente al responsable sus datos personales, de forma activa y consciente, lo cual incluye los datos personales obtenidos en el contexto del uso, la prestación de un servicio o la realización de un trámite, o bien, aquellos proporcionados por el titular a través de un dispositivo tecnológico;
- La portabilidad de los datos personales no afecte los derechos y libertades de terceros, y
- Cuando exista una relación jurídica entre el responsable receptor y el titular; se dé cumplimiento a una disposición legal, o bien, el titular pretenda ejercer algún derecho.

Lo anterior con excepción de la información indicada de acuerdo con el artículo 9 de los citados Lineamientos, misma que no será objeto de portabilidad.

Para efecto de lo señalado en el párrafo anterior, no será objeto de portabilidad de datos personales la siguiente información:

- Aquella inferida, derivada, creada, generada u obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionados directamente por el titular, como es el caso de los datos que hubieren sido sometidos a un proceso de personalización, recomendación, categorización, creación de perfiles u otros procesos similares o análogos;
- Los pseudónimos salvo que éstos se encuentren claramente vinculados al titular y puedan identificarlo o lo hagan identificable cuando el responsable cuente con información adicional que permita su individualización e identificación, y
- Los datos personales sujetos a un proceso de disociación, de tal manera que no puedan asociarse al titular ni permitir la identificación del mismo, salvo aquellos datos personales que por medio de un procedimiento posterior se puedan asociar de nuevo al titular.

El responsable deberá informar a los titulares sobre la posibilidad que tiene de solicitar la portabilidad de sus datos y su alcance, así como los tipos o categorías de datos personales que técnicamente sean portables; el o los tipos de formatos estructurados y comúnmente utilizados disponibles para

obtener o transmitir sus datos personales[151], y los mecanismos, medios y procedimientos disponibles para que el titular pueda solicitar la portabilidad de sus datos personales, a través del aviso de privacidad integral[152].

Respecto de la solicitud de portabilidad de datos personales, y de acuerdo con el artículo 15 de los Lineamientos de Portabilidad, en ésta no se podrán imponer mayores requisitos que los siguientes:

- La petición de solicitar una copia de los datos personales;
- La explicación general de la situación de emergencia en la que se encuentra el titular, en su caso, y
- La denominación del responsable y el documento que acredite la relación jurídica entre el responsable y el titular.

El titular podrá acompañar a su solicitud el medio de almacenamiento para la elaboración de la copia correspondiente y en caso de que el titular no lo proporcione, el responsable deberá facilitarlo.

La portabilidad deberá ser gratuita salvo el costo razonable del medio de almacenamiento a través del cual se entregue la copia de los datos. El costo antes mencionado deberá atender a las especificaciones establecidas en el artículo 20 de los Lineamientos de Portabilidad.

Para llevar a cabo la portabilidad de datos, el responsable deberá realizar al menos las siguientes acciones y actividades[153]:

- Implementar mecanismos, medios y procedimientos idóneos que permitan al titular obtener sus datos personales, sea de manera personal, por vía electrónica, a través de opciones de descarga establecidas en sus portales de internet, o por cualquier otra tecnología que considere pertinente;
- Informar al titular sobre el o los tipos de formatos estructurados y comúnmente utilizados disponibles a través de los cuales podrá entregar o transmitir los datos personales al responsable receptor;
- Garantizar la interoperabilidad tanto de los formatos estructurados y comúnmente utilizados en el que se entreguen los datos personales, así como de los servicios y sistemas electrónicos, y

[151] Artículo 11 de los Lineamientos de Portabilidad.
[152] Artículo 28 de la Ley General.
[153] Artículo 25, fracciones I y II de los Lineamientos de Portabilidad.

- Procurar que los servicios y sistemas electrónicos en su posesión mantengan la capacidad de interoperar con otros sistemas.[154]

Respecto de las Condiciones técnicas para la transmisión de datos personales, los responsables deben observar lo siguiente:

- Adoptar protocolos, herramientas, aplicaciones o servicios que permitan el enlace y comunicación eficiente de los datos;[155]
- Establecer medidas de seguridad de carácter administrativo, físico y técnico para la transmisión de los datos personales como son, de manera enunciativa mas no limitativa, mecanismos de autenticación de usuarios, conexiones seguras, o bien, utilizar medios electrónicos de transmisión cifrados;[156]
- Establecer mecanismos de autenticación para el envío y recepción de los datos, los cuales deberán ser de uso exclusivo de las condiciones técnicas aplicables;[157]
- Establecer controles que les permitan obtener evidencia sobre el envío, recepción e integridad de los datos personales transmitidos, y[158]
- Los sistemas o plataformas electrónicas utilizadas para el envío y recepción de los datos personales deberán llevar un registro de todas las acciones u operaciones realizadas con las transmisiones de éstos como son, de manera enunciativa mas no limitativa, la persona que está autorizada para transmitir los datos personales; la fecha y hora en que se efectuó la transmisión; la fecha y hora en que se recibieron los datos personales en el sistema o plataforma electrónica; la persona autorizada para recibir los datos personales; si la transmisión fue exitosa o fallida y cualquier otra información que se genere con la misma.[159]

Una vez que se cumplan las condiciones técnicas mencionadas, los responsables deberán realizar el procedimiento que los Lineamientos de Portabilidad establecen en el artículo 27.

Esta variable, solo es aplicable en los casos que se sea factible realizar la portabilidad de datos personales, por llevar a cabo un tratamiento de estos por vía electrónica en un formato estructurado y comúnmente utilizado, en caso de no ser así, se deberá especificar en el cumplimiento del criterio 2.

---

[154] Artículo 25, fracciones III y IV de los Lineamientos de Portabilidad.
[155] Artículo 26, fracción I de los Lineamientos de Portabilidad.
[156] Artículo 26, fracción II de los Lineamientos de Portabilidad.
[157] Artículo 26, fracción III de los Lineamientos de Portabilidad.
[158] Artículo 26, fracción IV de los Lineamientos de Portabilidad.
[159] Artículo 26, fracción V de los Lineamientos de Portabilidad.

La información publicada en este apartado deberá cumplir con las *reglas generales de evaluación* establecidas en el presente documento.

Periodo de actualización:

Portabilidad de datos personales: Trimestral y cada vez que exista una modificación, los responsables tendrán hasta 10 días hábiles para actualizar la información.

Normas técnicas: Bianual y cada vez que exista una modificación, los responsables tendrán hasta 10 días hábiles para actualizar la información.

Condiciones técnicas: Bianual y cada vez que exista una modificación, los responsables tendrán hasta 10 días hábiles para actualizar la información.

Conservación: Se debe conservar la información vigente.

Ubicación en el sitio de internet del responsable: De conformidad con lo dispuesto en el artículo 250 de los Lineamientos Generales, la información relativa a la presente variable, así como los medios de verificación correspondientes a cada criterio de evaluación, deberán publicarse en el apartado "Protección de Datos Personales" del portal de internet del sujeto obligado, específicamente en la sección denominada "Información relevante en materia de protección de datos personales".

Criterios:

Formato 4.1 Portabilidad de datos personales

Ejercicio (año) del que se presenta la información		(AAAA)
Fecha de publicación de la información		(DD/MM/AAAA)
Fecha de la última actualización		(DD/MM/AAAA)
No.	**Criterio**	**Medio de verificación**
1.	Indique si el sujeto obligado realiza tratamientos de datos personales por medios automatizados o electrónicos (Sí / No) En caso de no realizar tratamientos de datos personales por medios automatizados o electrónicos, se deberá incluir la siguiente leyenda: "El/la (nombre del sujeto obligado) no realiza tratamiento de datos personales por medios automatizados o electrónicos." En caso de no hacerlo deberá omitir publicar información en los siguientes criterios de la presente variable	
2.	Señale si emplea un formato electrónico accesible y legible por medios automatizados, es decir, que éstos últimos pueden identificar, reconocer, extraer, explorar o realizar cualquier otra operación con datos personales específicos (Sí / No)	
3.	Indique si el formato utilizado permite la reutilización y/o aprovechamiento de los datos personales (Sí / No)	
4.	Documento que contenga el hipervínculo al / a los aviso(s) de privacidad integral(es) por cada tratamiento de datos personales en los cuales sea posible solicitar la portabilidad de estos, donde se establezcan los tipos o categorías de datos personales que	

	técnicamente sean portables; el o los tipos de formatos estructurados y comúnmente utilizados disponibles para obtener o transmitir sus datos personales, y los mecanismos, medios y procedimientos disponibles para que el titular pueda solicitar la portabilidad de sus datos personales. Dicho documento deberá contener la siguiente información[160]: a) Denominación del tratamiento de datos personales que permite la portabilidad b) Tipo de medio por el cual se difunde el aviso de privacidad (Físico / Electrónico / Físico y Electrónico / Óptico / Sonoro / Visual / Otra tecnología) c) Lugar físico en el cual el titular podrá revisar el aviso de privacidad d) Hipervínculo al aviso de privacidad publicado en el portal de internet del responsable	
5.	Señale si en caso de que el titular no acompañe a su solicitud el medio de almacenamiento para la elaboración de la copia correspondiente de sus datos personales, el sujeto obligado facilita dicho medio de almacenamiento (Sí / No)	
6.	Hipervínculo al documento mediante el cual establece las medidas de seguridad de carácter administrativo, físico y técnico para la transmisión de los datos personales como son, de manera enunciativa mas no limitativa, mecanismos de autenticación de usuarios, conexiones seguras, o bien, utilizar medios electrónicos de transmisión cifrados. **En caso de tratarse del documento de seguridad, deberá incluir la versión pública del mismo. Por ningún motivo debe incluirse en este apartado el documento de seguridad integro con el que cuenta el responsable. El documento de seguridad deberá publicarse protegiendo el plan de trabajo, el análisis de riesgo y el análisis de brecha respectivos; lo que implica que en caso de que se dejen visibles, sin excepción, será considerado como incumplimiento al presente criterio**	

Vertiente 5: Acciones preventivas en materia de protección de datos personales

Variable 5.1: Evaluación de impacto en la protección de datos personales

Con base en la Ley General, la evaluación de impacto en la protección de datos personales es *el documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable*[161].

La evaluación de impacto tiene por objeto[162]:

[160] Ver Anexo-Guía 6. Avisos de privacidad portabilidad.
[161] Artículo 3, fracción XVI de la Ley General.
[162] Artículo 7 de las Disposiciones para las evaluaciones de impacto.

- Identificar y describir los altos riesgos potenciales y probables que entrañen los tratamientos intensivos o relevantes de datos personales;
- Describir las acciones concretas para la gestión de los riesgos;
- Analizar y facilitar el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en la Ley General y demás disposiciones aplicables, respecto a tratamientos intensivos o relevantes de datos personales, y
- Fomentar una cultura de protección de datos personales al interior de la organización del responsable.

Al respecto y de acuerdo con el artículo 75 de la Ley General y artículos 8 y 9 de las Disposiciones para las evaluaciones de impacto, se deberá considerar como tratamiento intensivo o relevante de datos personales cuando:

- Existan riesgos inherentes a los datos personales a tratar;
- Se traten datos personales sensibles, y
- Se efectúen o pretendan efectuar transferencias de datos personales.

El documento correspondiente a la evaluación de impacto, deberá presentarse[163] al INAI de acuerdo con el contenido y especificaciones establecidas en las Disposiciones para las evaluaciones de impacto[164]; además, en caso de que el responsable tuviera dudas sobre la obligación de elaborar y presentar tal evaluación, podrá consultar directamente al INAI para que este realice una opinión técnica al respecto, o bien, hacer una consulta externa con los titulares o público involucrado en la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que pretenda implementar o modificar y que implique un tratamiento intensivo o relevante de datos personales, las cuales deberán ser documentadas y realizadas de acuerdo con lo establecido en los artículos 12 y 13 de las Disposiciones para las evaluaciones de impacto.

El contenido mínimo[165] de las evaluaciones de impacto es el siguiente:

- Descripción de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que pretenda poner en operación o modificar.[166]

[163] Artículo 74 de la Ley General.
[164] Artículo 76 de la Ley General.
[165] Artículo 14 de las Disposiciones para las evaluaciones de impacto.
[166] Artículo 15 de las Disposiciones para las evaluaciones de impacto.

- Justificación de la necesidad de implementarla.[167]
- Representación del ciclo de vida de los datos personales a tratar.[168]
- La identificación, análisis y descripción de la gestión de los riesgos inherentes.[169]
- Análisis del cumplimiento normativo.[170]
- Los resultados de las consultas externas que, en su caso, se hayan realizado.[171]
- La opinión técnica del Oficial de Protección de Datos Personales respecto del tratamiento intensivo o relevante.[172]
- Cualquier otra información que se considere conveniente hacer del conocimiento del INAI.

Las evaluaciones de impacto también podrán presentarse de manera interinstitucional, es decir, cuando dos o más responsables, de manera conjunta o coordinada, pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que, a su juicio y de conformidad con lo dispuesto en la Ley General, las Disposiciones para las Evaluaciones de Impacto y demás disposiciones aplicables en la materia, impliquen un tratamiento intensivo o relevante de datos personales, por lo que deberán elaborar de manera conjunta una sola evaluación que será presentada al INAI conforme a las siguientes reglas[173]:

- Si los responsables son del orden federal, la presentación de ésta se deberá hacer ante el INAI.
- Cuando se trate de un responsable del orden federal que de manera conjunta o coordinada con un responsable del orden estatal y/o municipal, la presentación de ésta se deberá hacer ante el Instituto y el organismo garante competente.

Al respecto, los responsables tendrán treinta días hábiles anteriores a la fecha en que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, ante el INAI a efecto de que éste emita las recomendaciones no vinculantes correspondientes, mediante un dictamen y dentro de los treinta días hábiles siguientes contados a partir del día hábil siguiente a la presentación de la evaluación[174].

[167] Artículo 17 de las Disposiciones para las evaluaciones de impacto.
[168] Artículo 18 de las Disposiciones para las evaluaciones de impacto.
[169] Artículo 19 de las Disposiciones para las evaluaciones de impacto.
[170] Artículo 20 de las Disposiciones para las evaluaciones de impacto.
[171] Artículo 21 de las Disposiciones para las evaluaciones de impacto.
[172] Artículo 22 de las Disposiciones para las evaluaciones de impacto.
[173] Artículo 11 de las Disposiciones para las evaluaciones de impacto.
[174] Artículo 28 de las Disposiciones para las evaluaciones de impacto.

El dictamen determinará de manera fundada y motivada alguno de los siguientes dos supuestos:

- Que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumple con lo dispuesto en la Ley General y demás normatividad aplicable y, por lo tanto, no será necesario emitir recomendaciones no vinculantes al respecto, o
- Que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales no cumple con lo dispuesto en la Ley General y demás normatividad aplicable y, por lo tanto, será necesario emitir recomendaciones no vinculantes.

Además, el INAI deberá pronunciarse respecto de[175]:

- Los controles y medidas que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos identificados;
- Los mecanismos o procedimientos que adoptará el responsable para que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumpla, desde el diseño y por defecto, con las obligaciones previstas en la Ley General y demás disposiciones aplicables, y
- La puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, en cuanto a la protección que de éstos se refiere.

Aunado a lo anterior, el dictamen emitido por el INAI podrá orientar al responsable para el fortalecimiento y mejor cumplimiento de las obligaciones previstas en la Ley General y demás disposiciones aplicables, señalando medidas, acciones y sugerencias específicas en función de las características generales y particularidades correspondientes.

Respecto de la exención[176] para la presentación de evaluaciones de impacto en la protección de datos personales, el responsable no deberá realizar y presentar una evaluación de impacto en la protección de datos personales cuando a su juicio:

[175] Artículo 29 de las Disposiciones para las evaluaciones de impacto.
[176] Artículo 79 de la Ley General y 33 de las Disposiciones para las evaluaciones de impacto.

- Se comprometan los efectos que se pretenden lograr con la posible puesta en operación o modificación de política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, o
- Se trate de situaciones de emergencia o urgencia.

Así, cuando el responsable identifique alguna de las situaciones anteriores, deberá presentar un informe al INAI durante los primeros treinta días hábiles posteriores[177] a la fecha de la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, contados a partir del primer día de la puesta en operación o modificación de ésta, a través del cual, de manera fundada y motivada, señale las características establecidas en el artículo 34 de las Disposiciones para las Evaluaciones de Impacto. Posteriormente, el INAI deberá analizar el informe en un plazo máximo de 15 días hábiles días contados a partir del día siguiente de su recepción y emitir una respuesta en los siguientes sentidos[178]:

- Determinando que la presentación de la evaluación de impacto en la protección de datos personales comprometía los efectos de política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que se pretender poner en operación o modificar;
- Reconociendo la situación de emergencia o urgencia planteada por el responsable, u
- Ordenando la presentación de la evaluación de impacto en la protección de datos personales por no actualizarse los supuestos a que se refieren los artículos 79 de la Ley General y 33 de las Disposiciones para las Evaluaciones de Impacto ante el INAI, en un plazo máximo de diez días hábiles contados a partir del día siguiente de la notificación de la respuesta.

Esta variable, solo es aplicable en los casos que el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología y que este implique un tratamiento intensivo o relevante de datos personales; en caso de no ser así, se deberá especificar en el cumplimiento del criterio 2.

[177] Artículo 34 de las Disposiciones para las evaluaciones de impacto.
[178] Artículo 37 de las Disposiciones para las evaluaciones de impacto.

La información se publicará a partir de que el responsable reciba la respuesta al informe de exención de evaluación de impacto emitida por el INAI.

La información publicada en este apartado deberá cumplir con las *reglas generales de evaluación* establecidas en las Disposiciones Generales del presente documento.

Periodo de actualización: Trimestral, o en su caso, cuando ocurra alguna actualización. El responsable tendrá hasta 10 días hábiles para actualizar la información.

Conservación: Se debe conservar la información vigente.

Ubicación en el sitio de internet del responsable: De conformidad con lo dispuesto en el artículo 250 de los Lineamientos Generales, la información relativa a la presente variable, así como los medios de verificación correspondientes a cada criterio de evaluación, deberán publicarse en el apartado "Protección de Datos Personales" del portal de internet del sujeto obligado, específicamente en la sección denominada "Información relevante en materia de protección de datos personales".

Criterios

Formato 5.1 Evaluación de impacto en la protección de datos personales

Ejercicio (año) del que se presenta la información		(AAAA)
Fecha de publicación de la información		(DD/MM/AAAA)
Fecha de la última actualización		(DD/MM/AAAA)
No.	**Criterio**	**Medio de verificación**
1.	Denominación de la política pública, programa, sistema, plataforma, aplicación o cualquier otra actividad que implique el tratamiento intensivo o relevante de datos personales realizado. En caso de que no aplique, el responsable deberá especificarlo y deberá omitir ingresar información en los criterios subsecuentes de la presente variable	
2.	La política pública, programa, sistema, plataforma, aplicación o cualquier otra actividad que implique el tratamiento intensivo o relevante de datos personales realizado está sujeta a alguna de	

	las exenciones de la presentación de evaluación de impacto (Sí/No)	
3.	En caso de una respuesta en sentido afirmativo, hipervínculo al informe de exención emitido por el INAI. Deberá omitir ingresar información en los criterios subsecuentes de la presente variable. En caso de que la política pública, programa, sistema, plataforma, aplicación o cualquier otra actividad que implique el tratamiento intensivo o relevante de datos personales realizado, no esté sujeta a alguna de las exenciones de la presentación de evaluación de impacto, publicar el hipervínculo a la evaluación de impacto entregada al INAI	
4.	Hipervínculo al dictamen de recomendaciones no vinculantes correspondiente emitido por el INAI	

Vertiente 6: Responsables en materia de Protección de Datos Personales

Variable 6.1: El Comité de Transparencia y la Unidad de Transparencia

El Comité de Transparencia[179] será la autoridad máxima en materia de protección de datos personales, al interior de cada responsable y tendrá las siguientes funciones[180]:

- Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con Ley General y demás normatividad aplicable en la materia;
- Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;
- Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;
- Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la Ley General y demás normatividad aplicable en la materia;
- Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
- Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto;
- Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y

[179] Artículo 43 de la Ley General de Transparencia.
[180] Artículo 84 de la Ley General.

- Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.

Todo responsable contará con una Unidad de Transparencia[181]. Para la designación del titular de la Unidad de Transparencia, el responsable deberá atender lo dispuesto en la Ley General de Transparencia.

La Unidad de Transparencia se integrará y funcionará conforme a lo establecido en la Ley General de Transparencia, además que tendrá las siguientes funciones[182]:

- Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección datos personales;
- Gestionar las solicitudes para el ejercicio de los derechos ARCO;
- Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;
- Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;
- Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO,
- Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, y
- Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.

Para que las personas con algún tipo de discapacidad o grupos vulnerables, puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales[183], los responsables promoverán acuerdos con instituciones públicas especializadas, para auxiliarse, en la recepción, trámite y entrega de las respuestas a solicitudes de derechos ARCO, en lengua indígena, braille o

[181] Artículo 45 de la Ley General de Transparencia.
[182] Artículo 85 de la Ley General.
[183] Artículo 86 de la Ley General.

cualquier formato accesible correspondiente, que se requiera en atención al titular, pudiendo adoptar el responsable las medidas establecidas en los Lineamientos Generales[184].

Para el caso de las personas con alguna discapacidad, la Unidad de Transparencia del responsable procurará atender a cada uno de los titulares, de acuerdo con su situación particular[185].

La información publicada en la presente variable deberá guardar congruencia con lo publicado en las variables Mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones de la Ley General y demás disposiciones aplicables en la materia y Actividades interrelacionadas para establecer y mantener las medidas de seguridad.

La información publicada en este apartado deberá cumplir con las *reglas generales de evaluación* establecidas en el presente documento.

Periodo de actualización: Trimestral, o en su caso, cuando ocurra alguna actualización. El responsable tendrá hasta 10 días hábiles para actualizar la información.

Conservación: Se debe conservar la información vigente.

Ubicación en el sitio de internet del responsable: De conformidad con lo dispuesto en el artículo 250 de los Lineamientos Generales, la información relativa a la presente variable, así como los medios de verificación correspondientes a cada criterio de evaluación, deberán publicarse en el apartado "Protección de Datos Personales" del portal de internet del sujeto obligado, específicamente en la sección denominada "Información relevante en materia de protección de datos personales".

Criterios:

Formato 6.1. El Comité de Transparencia y la Unidad de Transparencia

Ejercicio (año) del que se presenta la información		(AAAA)
Fecha de publicación de la información		(DD/MM/AAAA)
Fecha de la última actualización		(DD/MM/AAAA)
No.	**Criterio**	**Medio de verificación**
1.	Indicar si cuenta con Comité de Transparencia (Sí/No) En caso de que la respuesta sea negativa deberá omitir ingresar información en los criterios subsecuentes del presente formato	
2.	Hipervínculo al documento que contenga los procedimientos internos establecidos e implementados que aseguren mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO	

[184] Artículo 85 de los Lineamientos Generales.
[185] Artículo 84 de los Lineamientos Generales.

3.	Hipervínculo a los criterios específicos establecidos por el Comité para la mejor observancia de la Ley General y de aquellas disposiciones aplicables en la materia	
4.	Hipervínculo al programa de capacitación y actualización de los servidores públicos del responsable establecido por el Comité	
5.	Indique si cuenta con Unidad de Transparencia (Sí/No). En caso de que la respuesta sea negativa deberá omitir ingresar información en los criterios subsecuentes de la presente variable	
6.	Señale si la Unidad de Transparencia es el área encargada de gestionar las solicitudes para el ejercicio de los derechos ARCO (SÍ / No)	
7.	Hipervínculo al documento que contenga los mecanismos establecidos por la Unidad de Transparencia para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados	
8.	Hipervínculo al documento mediante el cual el responsable da a conocer al público en general, los costos por la reproducción y envío de los datos personales que le sean solicitados, con base en lo establecido en las disposiciones normativas aplicables	
9.	Hipervínculo al documento que contiene los instrumentos aplicados para evaluar calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO	
10.	Hipervínculo al documento que enliste el o los acuerdos realizados con instituciones públicas especializadas para auxiliar en la recepción, trámite y entrega de las respuestas a solicitudes de datos personales, en lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente	

Vertiente 6: Responsables en materia de Protección de Datos Personales

Variable 6.2: Oficial de Protección de Datos Personales

La Ley General, establece que los responsables que en ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales relevantes o intensivos, podrán designar a un oficial de protección de datos personales, especializado en la materia, quien realizará las atribuciones mencionadas en el artículo 85 de la Ley General y formará parte de la Unidad de Transparencia.

El oficial de protección de datos personales será aquella persona que cuente con la jerarquía o posición dentro de la organización del responsable que le permita implementar políticas transversales en esta materia, además de atender a sus conocimientos, cualidades profesionales, experiencia en la materia de protección de datos personales, y, en su caso, a la o las certificaciones con que cuente la persona en materia de protección de datos personales[186].

Se considera que se está en presencia de un tratamiento intensivo o relevante de datos personales, cuando[187]:

[186] Artículo 121, segundo y tercer párrafos de los Lineamientos Generales.

[187] Artículo 75 de la Ley General del Datos, 120 de los Lineamientos Generales y 8 y 9 de las Disposiciones para las evaluaciones de impacto.

- Existen riesgos inherentes a los datos personales a tratar, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de titulares involucrados; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular, la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas;
- Se traten datos personales sensibles a los que se refiere el artículo 3, fracción X de la Ley General, entendidos como aquellos que se refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los 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, y
- Se efectúen o pretendan efectuar transferencias de datos personales a las que se refiere el artículo 3, fracción XXXII de la Ley General, según corresponda, entendidas como cualquier comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado, considerando con especial énfasis, de manera enunciativa más no limitativa, las finalidades que motivan éstas y su periodicidad prevista; las categorías de titulares involucrados; la categoría y sensibilidad de los datos personales transferidos; el carácter nacional y/o internacional de los destinatarios o terceros receptores y la tecnología utilizada para la realización de éstas.

Además de lo anterior, el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales podrá emitir criterios adicionales con sustento en parámetros objetivos que determinen que se está en presencia de un tratamiento intensivo o relevante de datos personales, en función de[188]:

- El número de titulares;
- El público objetivo;

[188] Artículo 76 de la Ley General.

- El desarrollo de la tecnología utilizada, y
- La relevancia del tratamiento de datos personales en atención al impacto social o, económico del mismo, o bien, del interés público que se persigue.

El oficial de protección de datos personales tendrá las siguientes atribuciones[189]:

- Asesorar al Comité de Transparencia respecto de los temas que sean sometidos a su consideración en materia de protección de datos personales;
- Proponer al Comité de Transparencia políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley General y los Lineamientos de Datos Personales;
- Implementar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley General y los Lineamientos de Datos Personales, previa autorización del Comité de Transparencia;
- Asesorar permanentemente a las áreas adscritas al responsable en materia de protección de datos personales;
- Realizar opiniones técnicas respecto de las evaluaciones de impacto que en su caso realice el responsable, y
- Las demás que determine el responsable y la normatividad que resulte aplicable.

Es importante que el responsable cuente con un oficial de protección de datos personales, al que refiere el segundo párrafo del artículo 85 de la Ley General, el cual establece sus funciones, así como las funciones consideradas en los artículos 121 y 122 de los Lineamientos Generales.

Para el caso que no se requiera la designación del oficial de protección de datos personales, debido a que el responsable no lleva a cabo tratamiento de datos personales relevantes o intensivos o no se cuente con los recursos para su designación, se sugiere valorar la posibilidad de designar a personal que asesore, realice propuestas y asista, al Comité de Transparencia y a la Unidad de Transparencia en el cumplimiento de sus obligaciones en materia de protección de datos personales, el personal deberá contar con conocimientos técnicos sobre el derecho de protección de datos personales.

Esta variable, solo es aplicable en los casos que se lleve a cabo un tratamiento de datos personales relevantes o intensivos, en caso de no ser así, se deberá especificar en el cumplimiento del criterio 3.

[189] Artículo 122 de los Lineamientos Generales y 22 de las Disposiciones para las evaluaciones de impacto.

La información publicada en la presente variable deberá guardar congruencia con lo publicado en la variable Evaluación de impacto en la protección de datos personales; del presente documento.
La información publicada en este apartado deberá cumplir con las *reglas generales de evaluación* establecidas en el presente documento.

Periodo de actualización: Trimestral, o en su caso, cuando ocurra alguna actualización. El responsable tendrá hasta 10 días hábiles para actualizar la información.
Conservación: Se debe conservar la información vigente.
Ubicación en el sitio de internet del responsable: De conformidad con lo dispuesto en el artículo 250 de los Lineamientos Generales, la información relativa a la presente variable, así como los medios de verificación correspondientes a cada criterio de evaluación, deberán publicarse en el apartado "Protección de Datos Personales" del portal de internet del sujeto obligado, específicamente en la sección denominada "Información relevante en materia de protección de datos personales".

Criterios:

Formato 6.2. Oficial de Protección de Datos Personales

Ejercicio (año) del que se presenta la información		(AAAA)
Fecha de publicación de la información		(DD/MM/AAAA)
Fecha de la última actualización		(DD/MM/AAAA)
No.	**Criterio**	**Medio de verificación**
1.	Lleva a cabo tratamientos de datos personales intensivos o relevantes (Sí/No)	
2.	Hipervínculo al documento mediante el cual el responsable designó al Oficial de protección de datos personales	

Capítulo III. Indicadores

Descripción de los indicadores

Los indicadores contenidos en el presente documento se medirán de acuerdo con lo que a continuación se establece:

Formato genérico de ficha técnica

Ficha técnica de los Indicadores correspondientes a los índices de vertientes, variables y formatos	
Indicador	Índice de cumplimiento
Unidad Administrativa responsable del indicador	Dirección General de Evaluación, Investigación y Verificación del Sector Público (DGEIVSP)
Tipo de información	Medios de verificación documentales que se utilicen en los ejercicios de evaluación del desempeño respecto del cumplimiento de la Ley General y demás disposiciones que resulten aplicables en la materia.
Objetivo del indicador	
Asegurar/Proporcionar un medio para medir el cumplimiento de principios, deberes y obligaciones establecidos en la Ley General y demás disposiciones aplicables en la materia, a través de los medios de verificación publicados por los responsables.	
Descripción del indicador	
Medir el desempeño de los responsables respecto del cumplimiento de la Ley General y demás disposiciones aplicables en la materia, mediante formatos que aseguren que la organización, presentación y publicación de la información y/o documentos solicitados, sea la idónea para que el INAI evalúe los medios de verificación de principios, deberes y obligaciones establecidos en la Ley en cuestión.	
Datos de identificación del indicador	
Dimensión	Eficacia
Sentido del indicador	Ascendente; es decir, que el desempeño de los responsables respecto del cumplimiento de la Ley General, y demás disposiciones aplicables en la materia, represente un resultado positivo, de acuerdo con la meta que se establezca eventualmente.
Línea base y metas	
Línea base	Al tratarse de un instrumento técnico de evaluación sin precedentes que permite al INAI cumplir con sus atribuciones y funciones en materia de evaluación del desempeño establecidas en los artículos 89, fracción XXV de la Ley General; 246, 247, 248, 249, 250, 251, 252 y 253 de los Lineamientos Generales y 41 Bis, fracciones XII, XIII, XIV, XV, XVI y XVII del Estatuto Orgánico, no se cuenta con referencia alguna de resultados obtenidos por la medición de indicadores de evaluación del desempeño de los responsables respecto del cumplimiento de los principios, deberes y obligaciones, establecidos en la Ley General y demás disposiciones aplicables en la materia; por lo que, derivado de los eventuales resultados, se establecerá el valor de línea base de acuerdo con lo alcanzado.
Meta	Al tratarse de un instrumento técnico de evaluación, sin precedentes que permite al INAI cumplir con sus atribuciones y funciones en materia de evaluación del desempeño establecidas en los artículos 89, fracción XXV de la Ley General; 246, 247, 248, 249, 250, 251, 252 y 253 de los Lineamientos Generales y 41 Bis, fracciones XII, XIII, XIV, XV, XVI y XVII del Estatuto Orgánico, no se cuenta con referencia alguna de resultados obtenidos por la

	medición de indicadores de evaluación del desempeño de los responsables respecto del cumplimiento de los principios, deberes y obligaciones, establecidos en la Ley General y demás disposiciones aplicables en la materia; por lo que, derivado de los eventuales resultados, se establecerá la meta de acuerdo con lo alcanzado.
Tipo de valor de la meta	Relativo
Fórmula	
$$Indice\ de\ cumplimiento\ (j) = \sum_{i=1}^{n} \left(\frac{X}{n}\right)$$ **Valores de la fórmula:** *X*= Sumatoria de índice [simple/global] de cumplimiento [de vertiente, variable o formato] o, número de criterios dentro del formato (según corresponda) *n*= número de [vertientes, variables, formatos o criterios] que integran [la vertiente, variable o formato] j= componente bajo análisis (Vertiente, Variable, Formato o Criterio) *Los resultados de los índices serán expresados en porcentaje.*	
Nombre del indicador	Corresponde al indicador y el nombre del índice al cual se refiere
Medio de verificación	La información publicada en el apartado virtual "Protección de Datos Personales", sitio en el cual todos los responsables deben poner a disposición del Instituto y de los titulares y mantener actualizada la información correspondiente a los medios de verificación para acreditar el cumplimiento de principios, deberes y obligaciones establecidos en la Ley General y demás disposiciones aplicables en la materia.
Unidad de medida	Porcentaje del cumplimiento de los criterios establecidos en las vertientes, variables y formatos que conforman los instrumentos técnicos para la evaluación, aprobados por el Pleno del INAI.
Frecuencia de medida	
De acuerdo con el Programa Anual de Evaluación que apruebe el Pleno del INAI del ejercicio anual que corresponda.	
Método de recolección	
Revisión del apartado virtual "Protección de Datos Personales", ubicado en el Portal de internet de cada responsable y el que, en su caso, establezca el correspondiente Programa Anual de Evaluación aprobado por el Pleno del INAI.	

Las fichas técnicas de los indicadores de cada vertiente, variable y formato pueden ser consultadas en el Anexo 7 del presente documento.

Los índices simples de cumplimiento son los siguientes:

<table>
<tr><td rowspan="14">Índices

Simples

de cumplimiento</td><td colspan="2">Índice simple de cumplimiento del formato Apartado virtual “Protección de datos personales”</td></tr>
<tr><td colspan="2">Índice simple de cumplimiento de la vertiente 1: Principios</td></tr>
<tr><td>Índice simple de cumplimiento de la variable 1.1: Aviso de privacidad integral</td><td>Índice simple de cumplimiento del formato 1.1 Aviso de privacidad integral</td></tr>
<tr><td>Índice simple de cumplimiento de la variable 1.2: Mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones de la Ley General y demás disposiciones aplicables</td><td>Índice simple de cumplimiento del formato 1.2 Mecanismos para acreditar el cumplimiento de principios, deberes y obligaciones de la Ley General y demás disposiciones aplicables</td></tr>
<tr><td colspan="2">Índice simple de cumplimiento de la vertiente 2: Deberes</td></tr>
<tr><td>Índice simple de cumplimiento de la variable 2.1: Deber de seguridad</td><td>Índice simple de cumplimiento del formato 2.1 Deber de seguridad</td></tr>
<tr><td>Índice simple de cumplimiento de la variable 2.2: Deber de confidencialidad y comunicaciones de datos personales</td><td>Índice simple de cumplimiento del formato 2.2 Deber de confidencialidad y comunicaciones de datos personales</td></tr>
<tr><td colspan="2">Índice simple de cumplimiento de la vertiente 3: Ejercicio de los derechos ARCO</td></tr>
<tr><td>Índice simple de cumplimiento de la variable 3.1: Mecanismos para el ejercicio de los derechos ARCO</td><td>Índice simple de cumplimiento del formato 3.1 Mecanismos para el ejercicio de los derechos ARCO</td></tr>
<tr><td colspan="2">Índice simple de cumplimiento de la vertiente 4: Portabilidad</td></tr>
<tr><td>Índice simple de cumplimiento de la variable 4.1: Portabilidad de datos personales</td><td>Índice simple de cumplimiento del formato 4.1. Portabilidad de datos personales</td></tr>
<tr><td colspan="2">Índice simple de cumplimiento de la vertiente 5: Acciones preventivas en materia de protección de datos personales</td></tr>
<tr><td>Índice simple de cumplimiento de la variable 5.1: Evaluación de impacto en la protección de datos personales</td><td>Índice simple de cumplimiento del formato 5.1 Evaluación de impacto en la protección de datos personales</td></tr>
</table>

	Índice simple de cumplimiento de la vertiente 6: Responsables en materia de Protección de Datos Personales	
	Índice simple de cumplimiento de la **variable 6.1:** El Comité de Transparencia y la Unidad de Transparencia	Índice simple de cumplimiento del **formato 6.1.** Comité de Transparencia y la Unidad de Transparencia
	Índice simple de cumplimiento de la **variable 6.2:** Oficial de Protección de Datos Personales	Índice simple de cumplimiento del **formato 6.2.** Oficial de Protección de Datos Personales

El índice simple general de cumplimiento es el siguiente:

Índice simple general de cumplimiento (Se integra por:)	Índice simple de cumplimiento del formato Apartado virtual "Protección de datos personales"
	Índice simple de cumplimiento de la vertiente 1: Principios
	Índice simple de cumplimiento de la vertiente 2: Deberes
	Índice simple de cumplimiento de la vertiente 3: Ejercicio de los derechos ARCO
	Índice simple de cumplimiento de la vertiente 4: Portabilidad
	Índice simple de cumplimiento de la vertiente 5: Acciones preventivas en materia de protección de datos personales
	Índice simple de cumplimiento de la vertiente 6: Responsables en materia de Protección de Datos Personales

Los índices globales de cumplimiento son los siguientes:

Índices Globales de cumplimiento	Índice global de cumplimiento del formato Apartado virtual "Protección de datos personales"		
	Índice global de cumplimiento de la vertiente 1: Principios		
	Índice global de cumplimiento de la **variable 1.1:** Aviso de privacidad integral	Índice global de cumplimiento del **formato 1.1.** Aviso de privacidad integral	Índice global de cumplimiento de cada **criterio que integra el formato 1.1.** Aviso de privacidad integral
	Índice global de cumplimiento de la **variable 1.2:** Mecanismos para acreditar el cumplimiento de principios, deberes y	Índice global de cumplimiento del **formato 1.2** Mecanismos para acreditar el cumplimiento de principios, deberes y	Índice global de cumplimiento de cada **criterio que integra el formato 1.2** Mecanismos para acreditar el cumplimiento de principios, deberes y

	obligaciones de la Ley General y demás disposiciones aplicables	obligaciones de la Ley General y demás disposiciones aplicables	obligaciones de la Ley General y demás disposiciones aplicables
	Índice global de cumplimiento de la vertiente 2: Deberes		
	Índice global de cumplimiento de la **variable 2.1:** Deber de seguridad	Índice global de cumplimiento del **formato 2.1** Deber de seguridad	Índice global de cumplimiento de cada **criterio que integra el formato 2.1** Deber de seguridad
	Índice global de cumplimiento de la **variable 2.2:** Deber de confidencialidad y comunicaciones de datos personales	Índice global de cumplimiento del **formato 2.2** Deber de confidencialidad y comunicaciones de datos personales	Índice global de cumplimiento de cada **criterio que integra el formato 2.2** Deber de confidencialidad y comunicaciones de datos personales
	Índice global de cumplimiento de la vertiente 3: Ejercicio de los derechos ARCO		
	Índice global de cumplimiento de la **variable 3.1:** Mecanismos para el ejercicio de los derechos ARCO	Índice global de cumplimiento del **formato 3.1**Mecanismos para el ejercicio de los derechos ARCO	Índice global de cumplimiento de cada **criterio que integra el formato 3.1** Mecanismos para el ejercicio de los derechos ARCO
	Índice global de cumplimiento de la vertiente 4: Portabilidad		
	Índice global de cumplimiento de la **variable 4.1:** Portabilidad de datos personales	Índice global de cumplimiento del **formato 4.1.** Portabilidad de datos personales	Índice global de cumplimiento de cada **criterio que integra el formato 4.1** Portabilidad de datos personales
	Índice global de cumplimiento de la vertiente 5: Acciones preventivas en materia de protección de datos personales		
	Índice global de cumplimiento de la **variable 5.1:** Evaluación de impacto en la protección de datos personales	Índice global de cumplimiento del **formato 5.1** Evaluación de impacto en la protección de datos personales	Índice global de cumplimiento de cada **criterio que integra el formato 5.1** Evaluación de impacto en la protección de datos personales
	Índice global de cumplimiento de la vertiente 6: Responsables en materia de Protección de Datos Personales		
	Índice global de cumplimiento de la **variable 6.1:** El Comité	Índice global de cumplimiento del **formato 6.1** Comité de	Índice global de cumplimiento de cada **criterio que integra el**

	de Transparencia y la Unidad de Transparencia	Transparencia y la Unidad de Transparencia	**formato 6.1** Comité de Transparencia y la Unidad de Transparencia
	Índice global de cumplimiento de la **variable 6.2:** Oficial de Protección de Datos Personales	Índice global de cumplimiento del **formato 6.2** Oficial de Protección de Datos Personales	Índice global de cumplimiento de cada **criterio que integra el formato 6.2** Oficial de Protección de Datos Personales

El índice global de cumplimiento de protección de datos personales es el siguiente:

Índice global de cumplimiento protección de datos personales (Se integra por:)	Índice global de cumplimiento del formato Apartado virtual "Protección de datos personales"
	Índice global de cumplimiento de la vertiente 1: Principios
	Índice global de cumplimiento de la vertiente 2: Deberes
	Índice global de cumplimiento de la vertiente 3: Ejercicio de los derechos ARCO
	Índice global de cumplimiento de la vertiente 4: Portabilidad
	Índice global de cumplimiento de la vertiente 5: Acciones preventivas en materia de protección de datos personales
	Índice global de cumplimiento de la vertiente 6: Responsables en materia de Protección de Datos Personales

El cálculo de los índices de cumplimiento se realizará por medio de la HEPDP.

VII. Anexos

Anexo 1. Anexo- Guía 1. Información sobre el aviso o los avisos de privacidad integrales.

Anexo 2. Anexo- Guía 2. Instrumentos jurídicos que regulan la relación con los encargados con cláusula general de guardar confidencialidad.

Anexo 3. Anexo- Guía 3. Instrumentos jurídicos mediante los cuales se formaliza la contratación o adhesión a servicios, aplicaciones e infraestructura en el cómputo en la nube y otras materias.

Anexo 4. Anexo- Guía 4. Trasferencias de datos personales.

Anexo 5. Anexo- Guía 5. Información sobre derechos ARCO.

Anexo 6. Anexo- Guía 6. Avisos de privacidad portabilidad.

Anexo 7. Fichas técnicas e indicadores.

Anexo 8. Formatos obligatorios para publicación de medios de verificación.