

POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE DATOS PERSONALES

Objetivo:

El presente documento tiene como objetivo implementar los principios y deberes en materia de protección de datos personales en los procesos internos de gestión y tratamiento de datos personales que administre el Instituto Nacional de Cancerología en lo subsecuente INCan, conforme a lo previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSSO) y los Lineamientos de Protección de Datos Personales para el Sector Público.

Ámbito de Aplicación:

El presente documento es de aplicación y observancia general, así como obligatoria para todas las personas servidoras públicas del Instituto Nacional de Cancerología, que conforme a sus atribuciones realicen tratamiento de datos personales.

Disposiciones Generales:

1. Se debe realizar el tratamiento de datos personales con base en las atribuciones conferidas a cada una de las áreas del INCan establecidas dentro del marco legal en la materia y del consentimiento de la persona titular.
2. Previo a recabar datos personales, se debe mostrar el aviso de privacidad, y debe encontrarse en un lugar visible.
3. Al momento de recabar datos personales, se deberá hacer del conocimiento de la persona titular la finalidad por la cual se reciben.
4. Las áreas solo deberán tratar los datos personales que resulten estrictamente necesarios para el ejercicio de sus atribuciones y funciones.
5. Se deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que se reciban en ejercicio de las atribuciones otorgadas a las áreas del INCan.
6. Es obligación de todas las personas servidoras públicas del INCan que administren, actualicen o tengan acceso a bases de datos personales, conservar, manejar y mantener de manera estrictamente confidencial dicha información y no revelarla a terceros.
7. Cuando se recaben datos personales de menores de edad se deberá obtener el consentimiento expreso de quien o quienes ejerzan la patria potestad o tutela sobre éstos.
8. Las áreas deberán identificar todos los avisos de privacidad que se requieren, según los tratamientos que realicen.
9. Los avisos de privacidad deberán contener todos los elementos informativos que exige la norma, además de estar redactados de manera clara y sencilla.
10. A través de la Unidad de Transparencia, se deberá verificar que todas las áreas que recaben datos personales difundan los avisos de privacidad en el portal de internet del INCan en el apartado de

Protección de Datos Personales y estar disponibles de manera impresa en aquellas áreas que así lo ameriten, en un lugar visible y de fácil consulta por parte de las personas titulares.

De los principios, deberes y demás obligaciones del responsable:

Se deberá dar cumplimiento a lo siguiente:

Principio de licitud. Los datos personales tienen que ser tratados de manera lícita, es decir, debe sujetarse a las facultades o atribuciones que la normatividad aplicable le otorga.

Las áreas deberán considerar lo siguiente:

1. Revisar que los datos se traten conforme a la LGPDPPSO¹, Lineamientos Generales de Protección de Datos Personales para el Sector Públicos y demás normativa aplicable.
2. Conocer la normativa que en lo particular regule sus atribuciones, funciones y responsabilidades con relación al tratamiento de los datos personales que realice.
3. Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros, cuando así se requiera

Principio de lealtad. La obtención de los datos personales no podrá hacerse a través de medios engañosos, ni fraudulentos.

Las áreas deberán considerar lo siguiente:

1. Revisar los procedimientos y formatos utilizados para recabar datos personales, para verificar que en éstos no se utilicen prácticas que lleven a la obtención de los datos de manera dolosa, de mala fe o con negligencia.
2. Dar vista al Órgano Interno de Control en caso del uso de prácticas dolosas, de mala fe o negligentes para la obtención de los datos personales.
3. Respetar en todo momento la confianza razonable de privacidad de la persona titular de los datos personales.
4. Tratar los datos conforme a lo informado a la persona titular de los datos personales.
5. Verificar los tratamientos, a fin de confirmar que los mismos no den lugar a discriminación o trato injusto o arbitrario en contra del titular.
6. Elaborar avisos de privacidad con todos los elementos informativos que establece la LGPDPPSO, y con información que corresponda a la realidad del tratamiento que se efectúa.
7. Incluir en los avisos de privacidad todas las finalidades de los tratamientos, las cuales deberán estar redactadas de forma clara y sencilla.

Principio del consentimiento. Las áreas que realicen tratamiento de datos personales deberán contar con el consentimiento del titular para el tratamiento de sus datos personales, el cual deberá ir siempre ligado a las finalidades concretas del tratamiento que se informe en el aviso de privacidad.

¹ Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Las áreas deberán considerar lo siguiente:

1. Identificar las finalidades para las cuales se requiere el consentimiento de los titulares, que puede ser expreso² o tácito³.
2. Solicitar el consentimiento después de que se ponga a disposición del titular el aviso de privacidad.
3. Redactar las solicitudes de consentimiento de forma tal que éste sea libre, específico e informado, y que las solicitudes sean concisas y claras, estén en un lenguaje sencillo y acorde con el perfil del titular.
4. Definir el tipo de consentimiento que se requiere, según las categorías de datos personales que se vayan a tratar o las disposiciones normativas que regulen el tratamiento.
5. Habilitar los mecanismos necesarios para solicitar el consentimiento expreso.
6. Documentar la puesta a disposición del aviso de privacidad para la obtención del consentimiento tácito.
7. Solicitar el consentimiento previo a la obtención de los datos personales y después de la puesta a disposición del aviso de privacidad, cuando los datos personales se obtengan directamente de su titular o representante.
8. Cuando los datos personales no los proporcione directamente el titular o su representante, deberá enviar a los titulares el aviso de privacidad correspondiente al medio de contacto que tenga registrado. Asimismo, deberá informarles que cuentan con un plazo de 5 días hábiles para en su caso manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que requieran su consentimiento. Si el titular no manifiesta su negativa en el plazo de cinco días antes señalado, entonces podrá suponer que cuenta con el consentimiento tácito.
9. En el caso del consentimiento expreso, es necesario que el mismo se solicite, ya sea en el cuerpo del aviso de privacidad o en un instrumento aparte. No podrán tratar los datos personales si no cuenta con el consentimiento expreso del titular.

Principio de información. Las áreas que realizan tratamientos de datos personales se encuentran obligadas a informar a las personas titulares de los datos personales, a través de los avisos de privacidad, las características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

Las áreas deberán considerar lo siguiente:

1. Poner a disposición de los titulares el aviso de privacidad en los términos dispuestos en la LGPDPSO, y demás normativa aplicable.
2. Poner a disposición del titular el aviso de privacidad previo a la obtención de los datos personales, cuando éstos se obtengan de manera directa o personal del titular.

² En el caso del consentimiento expreso, por fuerza, el titular deberá indicar que consiente el tratamiento de sus datos personales, pues si no existe esa manifestación expresa, el responsable no podrá tratar los datos personales. En ese sentido, es necesario que el titular explícitamente diga que sí.

³ El consentimiento tácito se obtiene si el titular no se niega a que sus datos personales sean tratados, después de haber conocido el aviso de privacidad. Es decir, no es necesario que quede registrado que el titular autorizó el tratamiento de su información personal, sino que es suficiente con que no se niegue al tratamiento.

3. Poner a disposición de la persona titular el aviso de privacidad al primer contacto que se tenga con éste, cuando los datos personales se hayan obtenido de una transferencia consentida, de una que no requiera el consentimiento, o bien de una fuente de acceso público.
4. Poner a disposición del titular el aviso de privacidad previo a iniciar el uso de los datos personales para las nuevas finalidades (aprovechamiento), cuando requiera tratar los datos personales para finalidades distintas y no compatibles con aquéllas para las cuales los recabó inicialmente.
5. Redactar el aviso de privacidad de manera que sea claro, comprensible y con una estructura y diseño que facilite su entendimiento.
6. Comunicar el aviso de privacidad a encargados y/o a terceros que remita o transfiera datos personales.
7. Demostrar el cumplimiento del principio de información, en caso de que así se requiera.

Principio de proporcionalidad. Las áreas que realicen tratamiento de datos personales deberán tratar solo aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron.

Las áreas deberán considerar lo siguiente:

1. Tratar el menor número posible de datos personales.
2. Analizar y revisar que se soliciten sólo aquellos datos personales que resultan indispensables para cumplir con las finalidades de que se trate.
3. Cuando una normativa establezca con precisión los datos personales que deberán obtenerse para cumplir con la finalidad de que se trate, sólo deberán solicitarse dichos datos.

Principio de finalidad. Los datos personales sólo pueden ser tratados para cumplir con la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta. Se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales.

Las áreas deberán considerar lo siguiente:

1. Tratar los datos personales únicamente para la finalidad o finalidades que hayan sido informadas a la persona titular en el aviso de privacidad y, en su caso, consentidas por ésta.
2. Informar en el aviso de privacidad todas las finalidades para las cuales se tratarán los datos personales, y redactarlas de forma tal que sean determinadas.
3. Identificar y distinguir en el aviso de privacidad entre las finalidades primarias⁴ y secundarias⁵.
4. Ofrecer a la persona titular de los datos personales un mecanismo para que pueda manifestar su negativa al tratamiento de sus datos personales para todas o algunas de las finalidades secundarias.

⁴ Los datos personales que se recaben, son estrictamente necesarios para el servicio que se solicite.

⁵ Los datos personales no son necesarios para el servicio solicitado, pero pueden permitir y facilitar algún servicio adicional.

Principio de calidad. El principio de calidad significa que, deberán ser exactos, completos, pertinentes, actualizados y correctos,

Las áreas deberán considerar lo siguiente:

1. Adoptar las medidas que consideren convenientes para procurar que los datos personales cumplan con las características de calidad, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que la persona titular se vea afectada por dicha situación.
2. Conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos y el periodo de bloqueo.
3. Bloquear los datos personales antes de suprimirlos, y durante el periodo de bloqueo sólo tratarlos para su almacenamiento y acceso en caso de que se requiera determinar posibles responsabilidades en relación con el tratamiento de los datos personales.
4. Suprimir los datos personales, previo bloqueo, cuando haya concluido el plazo de conservación.

Principio de responsabilidad. A este principio se le conoce también como el principio de “rendición de cuentas”, ya que establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales.

Las áreas deberán considerar lo siguiente:

1. Cumplir con el programa de capacitación y actualización aprobado por el Comité de Transparencia.
2. Analizar los riesgos que implica todo tratamiento de datos personales.

Deber de confidencialidad. Este deber implica la obligación de guardar secreto respecto de los datos personales que son tratados. Este deber debe cumplirse para evitar causar un daño a su titular. De no ser así, un tercero no autorizado podría tener acceso a determinada información.

Las áreas deberán considerar lo siguiente:

1. Guardar confidencialidad en cualquier fase del tratamiento de los datos personales, incluso después de finalizar la relación con la persona titular.
2. Verificar que los encargados también guarden confidencialidad de los datos personales que tratan a nombre y por cuenta del responsable, aun después de concluida la relación con éste.
3. Capacitar al personal que tenga acceso y use información que contenga datos personales, para que conozca sus obligaciones con relación al tratamiento de datos personales.
4. Establecer procedimientos para evitar fuga de información o el acceso indebido a los datos personales.
5. Incluir en los contratos u otros instrumentos jurídicos que celebre con terceros, cláusulas de confidencialidad y para que quienes tengan acceso a los datos personales en posesión del responsable cumplan con esta obligación de confidencialidad.

6. Realizar verificaciones o supervisiones periódicas al trabajo realizado por los encargados, a fin de verificar que se cumplan con sus obligaciones en torno a la protección de los datos personales.

Deber de seguridad. Este deber se refiere a la obligación de establecer y mantener medidas de seguridad tanto técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Las áreas deberán considerar lo siguiente:

1. Establecer y mantener medidas de seguridad administrativas, físicas y técnicas.
2. No adoptar medidas de seguridad menores a aquéllas que mantengan para el manejo de su información.
3. Tomar en cuenta el riesgo inherente por tipo de dato personal; las posibles consecuencias para las personas titulares por una vulneración; la sensibilidad de los datos personales tratados y el desarrollo tecnológico.
4. Notificar a las personas titulares las vulneraciones de seguridad que se presenten, con la información y en el momento antes señalados;
5. Llevar a cabo las acciones correctivas que sean necesarias

Ciclo de vida de los datos personales

Obtención, uso y eliminación.

Las áreas que realizan tratamiento de datos personales deberán:

1. Identificar el flujo y ciclo de vida de los datos personales: por qué medio se recaban, en qué procesos se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen.
2. Elaborar un inventario de datos personales relacionando el tipo de tratamiento con el ciclo de vida.
3. Bloquear, cancelar, suprimir o destruir los datos personales, en los casos establecidos en la normatividad aplicable.

Roles y responsabilidades.

El artículo 33, fracción II de la LGPDPSO, establece que se deberán de definir los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales, conforme al sistema de gestión que cada área haya implementado.

Las funciones y obligaciones de las personas que tratan datos personales se han identificado en dos niveles:

- I. A nivel general, a través del Programa de Protección de Datos Personales del INCan, y conforme a las obligaciones que establece la Ley General y los Lineamientos Generales, estarán asociadas con el área responsable para su cumplimiento.

II. A nivel de servidor público, a través de los inventarios que se desarrollaron por cada uno de los tratamientos, en los cuales se identificó el personal que realiza el tratamiento, el área al que está adscrito y la finalidad de dicho tratamiento.

Sanciones.

Serán causas de sanción por incumplimiento de las obligaciones en materia de protección de datos personales, las establecidas en el artículo 163 de la LGPDPPSO:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;

II. Incumplir los plazos de atención para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente

y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;

VII. Incumplir el deber de confidencialidad;

VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la LGPDPPSO;

IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad;

X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGPDPPSO;

XI. Obstruir los actos de verificación de la autoridad;

XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la LGPDPPSO;

XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes; y

XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea;

PROCESO GENERAL PARA EL ESTABLECIMIENTO, ACTUALIZACIÓN, MONITOREO Y REVISIÓN DE LOS MECANISMOS Y MEDIDAS DE SEGURIDAD.

El artículo 33, fracción VII de la Ley General establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

De acuerdo con la fracción VI del artículo 35 de la Ley General, los mecanismos de monitoreo y revisión forman parte del documento de seguridad.

Así, respecto a los mecanismos de monitoreo y revisión de las medidas de seguridad, el artículo 63 de los Lineamientos Generales señala lo siguiente:

Monitoreo y supervisión periódica de las medidas de seguridad implementadas

Artículo 63. Con relación al artículo 33, fracción VII de la Ley General, el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua.

Para cumplir con lo dispuesto en el párrafo anterior del presente artículo, el responsable deberá monitorear continuamente lo siguiente:

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

Aunado a lo previsto en las fracciones anteriores del presente artículo, el responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

En este sentido, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad del INCan.

Mecanismos de Monitoreo

Se consideran los siguientes tipos de monitoreo:

1) Revisión de cumplimiento de las políticas internas, relacionadas con el tratamiento de datos personales, el cual tendrá el objetivo de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en proporción con lo dispuesto en la Ley General, los Lineamientos Generales, y demás normatividad que resulte aplicable.

Por lo cual, cada responsable cuando identifique algún cambio en los instrumentos antes mencionados, deberá realizar las siguientes actividades:

- a. Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.
- b. Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.
- c. Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.
- d. Revisar y, en su caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

2) Revisión del riesgo. El objetivo será de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ello, podrán implementar los siguientes monitoreos:

- a) Monitoreo del entorno físico. Para la detección continua de amenazas y vulnerabilidades en el entorno físico, actualmente se cuenta con:
- b) Personal de vigilancia en los accesos de cada una de las entradas a las instalaciones del INCan.
- c) Control de acceso con gafete de identificación que acredite ser personal que colabora en el INCan
- d) Control de acceso a través de bitácoras para visitantes.
- e) Control de acceso a través de bitácoras del personal del INCan que olvidó su credencial, en su caso)
- f) Control de asistencia a través de medios electrónico y/o bitácora de asistencia.
- g) Monitoreo del entorno electrónico. Para la detección continua de amenazas y vulnerabilidades, El Departamento de Tecnologías de la Información del INCan, deberá contar con herramientas automatizadas de monitoreo, así como con bitácoras de los sistemas informáticos.
- h) Actualización del plan de trabajo. Derivado del monitoreo del entorno físico o electrónico, se podrán realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios se pondrán a consideración del área en riesgo, el Departamento de Tecnologías de la Información y el Comité de Transparencia.
- i) Actualización tecnológica. Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, el Departamento de Tecnologías de la

Información, realizará una actualización del análisis de riesgo, análisis de brecha y plan de trabajo.

- j) Vulneraciones a la seguridad de los datos personales. En caso de identificar un incidente de seguridad que involucre datos personales en sistemas electrónicos, el área responsable con apoyo del Departamento de TI y apoyo del Comité de Transparencia se coordinarán para decidir sobre las acciones pertinentes para mitigar dicho incidente.

Plazos de Atención para el ejercicio de los Derechos Arco (Acceso, Rectificación, Cancelación y Oposición).

No competencia	3 días
Prevención	5 días
Respuesta del solicitante a la prevención	10 días
Plazo normativo para dar respuesta	20 días + 10 adicionales (aprobado por el Comité de Transparencia)