POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES DEL CONSEJO NACIONAL DE NORMALIZACIÓN Y CERTIFICACIÓN DE COMPETENCIAS LABORALES

INTRODUCCIÓN

El día 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, la cual tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de todo ente público de los tres órdenes de gobierno, en concordancia con los estándares internacionales y nacionales en la materia, con el fin de establecer los elementos mínimos e imprescindibles que permitan uniformar el derecho a la protección de datos personales en el país en el sector público.

Debido a lo anterior y con fundamento en el artículo 30, fracción II, de la Ley General en la materia, el Consejo Nacional de Normalización y Certificación de Competencias Laborales (CONOCER), como responsable de los datos personales que recaba y posee, ha desarrollado una Política de Protección de Datos Personales.

En general, todos los servidores públicos que laboran en el CONOCER que de forma manual o automatizada obtengan, usen, registren, organicen, conserven, elaboren, utilicen, comuniquen, difundan, almacenen, posean, accedan, manejen, aprovechen, transfieran o dispongan de los datos personales deberán de observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; de igual forma, siempre deberán de apegar su actuar a lo mandatado en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los Lineamientos Generales de Protección de Datos Personales para el Sector Público, los acuerdos y criterios que emita el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y la presente Política interna.

I GLOSARIO DE TÉRMINOS.

- **Bases De Datos:** Conjunto ordenado de datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, 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;

- **Catálogo De Bases De Datos Personales:** Lista detallada del conjunto ordenado de bases datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u

holográfico, 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;

- **Datos Personales:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, 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;

- **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;

- **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;

- **CONOCER**: Consejo Nacional de Normalización y Certificación de Competencias Laborales;

- **Inventario De Datos Personales:** Lista ordenada y detallada que posea el responsable o encargado, de cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable;

- **Ley General:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO);

- **Ley Federal:** Ley Federal de Protección de Datos Personales en Posesión de los Particulares;

- **Reglamento:** Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;

- **Medidas De Seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;

- **Medidas De Seguridad Administrativas:** Políticas, acciones 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;

- **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 como prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información.

- **Medidas De Seguridad Técnicas:** Conjunto de acciones, mecanismos y sistemas de los datos personales y los recursos involucrados en su tratamiento como revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

- **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;

- **Titular:** La persona física a quien corresponden los datos personales;

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

II DE LOS SERVIDORES PÚBLICOS QUE TRATAN DATOS PERSONALES

Todo servidor público que trate datos personales dentro del CONOCER deberá de observar lo mandatado en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, sus respectivos lineamientos, la legislación vigente en la materia; así como lo señalado en la Política de Protección de Datos Personales del CONOCER.

III DE LA RECOLECCIÓN Y USO DE LOS DATOS PERSONALES

Los servidores públicos dentro de este Sujeto Obligado deberán de tratar los datos personales que posean sujetándose a las atribuciones y/o facultades que la normatividad

aplicable les confiera y siempre ese tratamiento deberá de estar justificado por finalidades concretas, lícitas, explícitas y legítimas.
Jamás se podrán obtener y tratar datos personales, a través de medios engañoso o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad. Por lo que obtener el consentimiento previo del titular para tratar los datos personales es esencial; y deberá ser otorgado de manera libre, específica e informada, siguiendo la normatividad aplicable.

Cuando se recaben los datos personales de los titulares, siempre se deberá de observar que los mismos resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifique su tratamiento.

Los datos personales que posean los servidores públicos deberán de ser exactos, correctos, completos y actualizados, de tal forma que no se pudiera afectar la veracidad de los mismos, su integridad permita el cumplimiento de las finalidades que motivaron su tratamiento y respondan fielmente a la situación actual del titular. Por lo que será necesario que se establezca y documente un procedimiento para la conservación, bloqueo y supresión de los datos personales. En los procedimientos de supresión de datos se deberá de contemplar la irreversibilidad del procedimiento, la seguridad y confidencialidad dentro de la eliminación y que los mecanismos utilizados sean favorables al medio ambiente.

Cumpliendo con el principio de información, los servidores públicos que recaben datos personales deberán de informar a los titulares, por medio del aviso de privacidad, la existencia y las características principales del tratamiento al que serán sometidos los mismos.

El aviso de privacidad deberá ponerse a disposición del titular en dos modalidades, la simplificada y la integral, cumpliendo con la legislación vigente, conforme a las siguientes reglas:

a) De forma previa a la obtención de los datos personales, cuando los mismos se obtengan directamente del titular, independientemente de los formatos o medios físicos y/o electrónicos utilizados para tal fin, y

b) Al primer contacto con el titular o previo al aprovechamiento de los datos personales, cuando éstos se hubieren obtenido de manera indirecta del titular.

Para la publicación de los avisos de privacidad se deberá considerar el perfil de los titulares, la forma en que mantiene contacto o comunicación con los mismos, que sean gratuitos, de fácil acceso, con la mayor cobertura posible y que se encuentren debidamente habilitados y disponibles en todo momento.

Con relación al aviso de privacidad integral, éste tendrá que estar publicado de manera permanente, en el sitio o medio que se informe en el aviso de privacidad simplificado, a

efecto de que el titular lo pueda consultar en cualquier momento y el INAI pueda acreditar tal situación fehacientemente.
El aviso de privacidad deberá ser elaborado por la Dirección correspondiente que recabe los datos y éste tendrá que realizarse por procedimiento, por lo que existirán tantos avisos como procedimientos en los que se recaben datos personales. Los avisos de privacidad podrán ser enviados a la Unidad de Transparencia con el objetivo de que ésta proporcione observaciones y/o sugerencias técnico-jurídicas; pero cada Dirección validara sus propios avisos de privacidad.

IV DE LOS DEBERES DE PROTECCIÓN PARA LOS DATOS PERSONALES

Con el objetivo de crear una eficiente protección y control de los datos personales dentro de su tratamiento, el CONOCER deberá de crear un sistema de gestión, el cual permita planificar, establecer, implementar, operar, monitorear, revisar y mejorar las medidas de seguridad de carácter administrativo, físico, y técnico aplicadas a los datos personales, tomando en consideración los estándares nacionales e internacionales en la materia.

El sistema de gestión deberá de integrarse tomando en cuenta los siguientes factores:

La documentación de las funciones, obligaciones, roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales dentro del procedimiento.

La señalización de las consecuencias del incumplimiento de las obligaciones y responsabilidades para con la protección de los datos.

Inventario de los datos personales, en el cual se deberá de contemplar como mínimo: 1) el catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales; 2) finalidades de cada tratamiento de los datos, 3) el catálogo de los tipos de datos que se tratan, indicando si son sensibles o no; 4) el catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y electrónica; 5) la lista de servidores públicos que tiene acceso a los sistemas de tratamiento; 6) el nombre completo del encargado, señalando el instrumento jurídico que formaliza la prestación de servicios y 7) los destinatarios o terceros receptores de las transferencia que se efectúen.

El ciclo de vida de los datos personales contemplando como mínimo: 1) la obtención de los datos personales; 2) el almacenamiento de los datos personales, 3) el uso de los datos conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin, 4) la divulgación de los datos personales considerando las remisiones y transferencias que en su caso se efectúen, 5) el bloqueo de los datos y en su caso la cancelación, supresión o destrucción de los datos personales.

La implementación de un análisis de riesgos, en el cual se deberá de tomar en cuenta las amenazas, vulnerabilidades, responsables, acciones a tomar en cuenta y consecuencias. La implementación de un análisis de brecha, en el cual se deberá reportar las medidas de seguridad existentes, efectivas y las medidas de seguridad faltantes.

El CONOCER deberá de implementar como mínimo medidas de seguridad, administrativas, físicas y técnicas, por procedimiento, en los cuales se traten datos personales; éstas deberán de realizarse atendiendo a la naturaleza de los datos tratados y plasmados en el documento de seguridad.

Aunado a lo anterior, deberá de evaluar y medir los resultados de sus sistemas de gestión anualmente, a fin de verificar el cumplimiento de los objetivos propuestos e implementar mejoraras continuas, esta evaluación también deberá de realizarse en caso de haberse presentado una vulneración dentro del sistema. La creación, implementación, monitoreo y supervisión de los distintos sistemas de gestión deberán de estar plasmados en un plan de trabajo que defina las acciones a realizarse, los servidores públicos responsables de su seguimiento y los términos para su implementación.

En caso de presentarse una vulneración dentro de las medidas de seguridad implementadas, el servidor público responsable del tratamiento de los datos deberá de activar las acciones preventivas y correctivas para evitar vulneraciones futuras de la misma índole, así como acciones para mitigar el daño al titular o titulares de los datos que se vieron afectados por la vulneración; asimismo, deberá de informarle al titular y al Órgano Garante la vulneración que se presentó, atendiendo a las obligaciones contempladas en los artículos 36, 37, 38, 39, 40 y 41 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 66, 67, 68 y 69 de los lineamientos en la materia. La vulneración dentro de las medidas de seguridad de algún procedimiento es una causal para realizar una evaluación y medición del sistema de gestión; así como la actualización del documento de seguridad.

Todos los servidores públicos que estén involucrados en el tratamiento de los datos personales dentro del sistema de gestión deberán de guardar confidencialidad de estos, aun después de haber finalizado su tratamiento y supresión de los mismos. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectué, por procedimiento se deberá de establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales que permita protegerlos contra daño, pérdida, alteración, destrucción o en su caso, acceso o tratamiento no autorizados.

Para la elaboración de cualquier medida se deberá de contemplar como mínimo lo siguiente:

- El riesgo inherente a los datos personales tratados;
- La sensibilidad de los datos;
- El desarrollo tecnológico de los datos;

- Las posibles consecuencias de una vulneración para los titulares;
- Las transferencias de datos personales que 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 autoriza para su posesión. En específico para las medidas de seguridad administrativas deberá de contemplarse como mínimo:
- Los procedimientos para la gestión, soporte y revisión de la seguridad de la información;
- La identificación, clasificación y borrado de la información y La sensibilización y capacitación del personal en la materia.

Respecto a las medidas de seguridad físicas deberá de contemplarse como mínimo:

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

Con relación a las medidas de seguridad técnicas se deberá de contemplar como mínimo lo siguiente:

- Prevención del 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 requiera con motivo de sus funciones;
- Revisión de 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 los datos.

Toda medida de seguridad que se elaboré deberá de estar plasmada dentro del documento de seguridad; así como las actualizaciones o sustituciones de las mismas. Las medidas tendrán que ser evaluadas anualmente o cuando exista una vulneración dentro de éstas.

Las Direcciones del CONOCER podrán someter a consideración de la Unidad de Transparencia las medidas de seguridad que implementarán, con el objetivo de que ésta vierta recomendaciones y/o sugerencias técnico-jurídicas.

El documento de seguridad deberá de ser elaborado de la siguiente forma y contemplando como mínimo lo siguiente:

1. Inventario de datos personales y sistemas de tratamiento: en este apartado se deberá de enunciar el catálogo de datos personales que son tratados según el sistema especificándose lo siguiente:
   a) El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales.
   b) Las finalidades de cada tratamiento de datos personales.
   c) El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no.
   d) El catálogo de formatos de almacenamiento así como la descripción general de la ubicación física y/ o electrónica de los datos personales.
   e) La lista de servidores públicos que tienen acceso a los sistemas de tratamiento.
   f) En su caso el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la presentación de los servicios que brinda al responsable.
   g) Si llegase a aplicar, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican éstas.

2. Ciclo de vida de los datos personales, el cual debe de contener:
   a) La obtención de los datos personales.
   b) El almacenamiento de los datos personales.

3. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/ o electrónicos utilizados para tal fin.

4. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen.

5. El bloqueo de los datos personales.

6. La cancelación, supresión o destrucción de los datos personales.

7. Las funciones y obligaciones de las personas que traten datos personales: se deberá establecer y documentar los roles y responsabilidades, así como la cadena de rendición de cuentas de todas las personas que traten datos personales en su organización, conforme al sistema implementado.

8. Explicación del sistema y políticas internas para la gestión y tratamiento de los datos personales: en este apartado se deberá de explicar brevemente cómo funciona el sistema o los sistemas y las políticas internas de seguridad que se utilicen.

9. Análisis de riesgo: para poder realizar este análisis deberá ser tomado en cuenta lo siguiente:

   a) Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector en específico.
   b) El valor de los datos personales de acuerdo a su clasificación previamente definida y a su ciclo de vida.
   c) El valor y exposición de los archivos involucrados en el tratamiento de los datos personales.
   d) Las consecuencias negativas para los titulares que pudieren derivar de una vulneración de seguridad ocurrida.
   e) El riesgo inherente a los datos personales tratados.
   f) La sensibilidad de los datos personales tratados.
   g) El desarrollo tecnológico.
   h) Las posibles consecuencias de una vulneración para los titulares.
   i) El número de titulares.
   j) Las vulneraciones previas ocurridas en los sistemas de tratamiento.
   k) El riesgo por el valor potencial cuantitativo o cualitativo que pudieren tener los datos personales tratados para una tercera persona no autorizada para su posesión.
   l) Explicación objetiva de las amenazas y vulnerabilidades posibles, así como del daño, posibles consecuencias y toma de acciones.

10. Análisis de brecha: para realizar este análisis deberá ser considerado lo siguiente:

    a) Las medidas de seguridad existente y efectiva.
        i. Físicas.
        ii. Administrativas.
        iii. Técnicas.
    b) Las medidas de seguridad faltantes.
        i. Físicas.
        ii. Administrativas.
        iii. Técnicas.
    c) Cómo se efectúan las transmisiones de datos personales.
    d) Uso de Bitácoras para acceso y operación cotidiana.
    e) Registro de incidentes.
    f) Uso de perfiles de usuario y contraseñas.
    g) Procedimientos de actualización de la información.
    h) Procedimientos de respaldo y recuperación de información.
    i) Plan de contingencia.

11. Monitoreo y supervisión de las medidas de seguridad: en este apartado se deberá evaluar y medir los resultados de las políticas, planes, proceso y procedimientos implementados en materia de seguridad y tratamiento de datos personales, a fin de verificar el cumplimiento con los objetivos propuestos; para poder desarrollar lo anterior se deberá contemplar lo siguiente:

    a) Los nuevos activos que se incluyen en la gestión de riesgos.
    b) Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras,
    c) Las nuevas amenazas que podrían estar activas dentro y fuera de la organización y que no hayan sido valoradas.
    d) La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
    e) Las vulnerabilidades identificadas para determinar aquellas expuestas a amenazas nuevas o pasadas que vuelven a surgir.
    f) El cambio en el impacto o consecuencia de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
    g) Los incidentes y vulneraciones de seguridad ocurridas.

12. Capacitación: la Unidad Administrativa deberá de implementar un programa de corto, mediano y largo plazo que tenga como objetivo el capacitar a los servidores públicos integrantes en materia de protección de datos personales, su tratamiento, y medidas de seguridad. Para realizar lo anterior, podrán pedirle apoyo a la Unidad de Transparencia.

13. Plan de trabajo: en este rubro se deberá de definir y señalar las acciones a implementar de acuerdo con el resultado del análisis de riesgo y de brecha, así como los demás apartados del documento.

V DE LA CAPACITACIÓN.

La Unidad de Transparencia designará a un enlace de capacitación ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y este enlace será el encargado de desarrollar un programa de capacitación anual en conjunto con la Unidad de Transparencia y dará seguimiento al mismo.

El programa se presentará al inicio de cada año al Comité de Transparencia; este podrá realizar las observaciones, recomendaciones o solicitudes que considere pertinentes y deberá aprobarlo.

El programa de capacitación presentado por la Unidad de Transparencia, deberá contemplar los roles y responsabilidades asignadas a las personas involucradas en el tratamiento de los datos, las medidas de seguridad implementadas, los perfiles de puesto, 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.

Una vez aceptado el programa de capacitación, la Unidad de Transparencia enviará a las Direcciones del CONOCER través de sus enlaces de capacitación, los cursos disponibles.

VI DEL EJERCICIO DE LOS DERECHOS ARCO

Las solicitudes para el ejercicio de los derechos Acceso, Rectificación, Cancelación y Oposición (ARCO) deberán presentarse ante la Unidad de Transparencia del CONOCER, a través de un escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto se establezca, en el ámbito de sus respectivas competencias.

La Unidad de Transparencia establecerá el procedimiento para el ejercicio de los derechos ARCO, el cual se encontrará para consulta en la sección de Protección de Datos Personales en la página web institucional del CONOCER.

VII DE RELACIÓN ENTRE EL RESPONSABLE Y EL ENCARGADO

El titular es la persona física a quien corresponden los datos personales; el responsable es el sujeto obligado, es decir, el CONOCER, quien decide sobre el tratamiento de datos personales y el encargado es 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; en todo momento el responsable y el encargado deberán de regirse bajo los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.

La relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normatividad que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido.

El encargado deberá realizar las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido de los mismos, así como limitar sus actuaciones a los términos fijados por el responsable.

El instrumento jurídico a través del cual se formalice la relación deberá de contener como mínimo lo siguiente con respecto a los servicios que preste el encargado:

1. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.
2. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.
3. Implementar las medidas de seguridad físicas, administrativas y técnicas conforme a los instrumentos jurídicos aplicables.
4. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.
5. Guardar confidencialidad respecto de los datos personales tratados.
6. Suprimir o 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.
7. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o de la comunicación derive una subcontratación, o por mandato expreso de la autoridad competente.
8. Permitirle al INAI o al responsable realizar verificaciones en el lugar o establecimiento donde lleve a cabo el tratamiento de los datos personales.
9. Colaborar con el INAI en las investigaciones previas y verificaciones.
10. Generar, actualizar y conservar la documentación necesaria para acreditar el complimiento de sus obligaciones.

El responsable también podrá contratar o adherirse a serv1c1os, aplicaciones e infraestructura en el computo 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 equivalente a los principios y deberes que observa e implementa el responsable de acuerdo a la normatividad aplicable.

En específico, en los servicios en los que el responsable se adhiera mediante condiciones o cláusulas generales de contratación, sólo podrá realizarlo con aquellos que el proveedor: I. Cumpla, al menos, con: a) tener y aplicar políticas de protección de datos personales a fines a los principios y deberes contemplados en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; b) transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio, c) 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 servicios y, d) guardar confidencialidad respecto de los datos personales a los que les de tratamiento.

2. Cuente con mecanismo para: a) dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) establecer y mantener medidas

de seguridad administrativas, físicas y técnicas de protección de los datos, d) garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último pueda recuperarlos e; e) impedir el acceso a los datos personales de personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada por autoridad competente.

En caso de que el encargado y subcontratado incumplan las obligaciones contraídas con el responsable, decidiendo y determinando, por si mismos, los fines, medios y demás cuestiones relacionadas con el tratamiento de los datos personales, asumirán el carácter de responsables.

VIII DEL COMITÉ DE TRANSPARENCIA

El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales y tendrá las funciones contempladas en las Leyes General de Transparencia y Acceso a la Información Pública, Federal de Transparencia y Acceso a la Información Pública y General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como los lineamentos aplicables.

IX DE LA UNIDAD DE TRANSPARENCIA

La Unidad de Transparencia asesorará a las Direcciones del CONOCER en materia de protección de datos personales; gestionará las solicitudes para el ejercicio de los derechos ARCO y podrá proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan la mayor eficiencia de la gestión de dichas solicitudes.