



Comisión Nacional  
de Hidrocarburos

S e p t i e m b r e 2 0 2 4

# Documento de Seguridad para la Protección de Datos Personales de la Comisión Nacional de Hidrocarburos

---

Comité de Transparencia de la  
Comisión Nacional de Hidrocarburos

## 1. Presentación

La Constitución Política de los Estados Unidos Mexicanos en los artículos 6o. y 16 incorpora el derecho de toda persona a la protección de sus datos personales, así como al acceso, rectificación, cancelación y oposición en los términos que determina la ley.

La Ley General de Protección de Datos Personales en Posesión de Sujetos obligados (LGPDPSSO) establece por su parte un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados.

A partir de lo anterior, el Documento de Seguridad tiene como propósito establecer el marco de referencia del tratamiento de los datos personales que se lleva a cabo al interior de la Comisión Nacional de Hidrocarburos (CNH) por las diversas unidades administrativas que conforman su estructura orgánica, para mantener vigente y promover la mejora continua en la protección de los mismos, en términos de lo previsto en los artículos 35 y 36 de la LGPDPSO, además de desarrollar buenas prácticas en la materia.

En ese sentido, la CNH ha identificado los procesos que en el ámbito de su competencia involucran el tratamiento de datos personales, a efecto de mantener la seguridad de los mismos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo a sus respectivos ámbitos de funciones.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión de la CNH, pues tal y como lo dispone el artículo 34 de la LGPDPSO, se entiende por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, operar, monitorear, mantener y mejorar el tratamiento y seguridad de los datos personales.

La CNH comprometida con la tutela de los datos personales que trata y en consonancia con la recomendación emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), ha impulsado a su interior las acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizados a los datos, mediante la implementación de medidas físicas, administrativas y técnicas, tendentes a garantizar la seguridad e integridad de los mismos, así como su seguimiento y supervisión continuos.

El Sistema permita disponer de información relacionada con las medidas de seguridad, el análisis general de las amenazas y posibles vulnerabilidades, así como los mecanismos o acciones a implementar para mitigarlas.

El presente documento se integra a partir de la gestión de actividades coordinadas para controlar y verificar que el tratamiento de los datos personales sea acorde con los principios que rigen su protección, pues para la CNH la política de seguridad en esta materia constituye un compromiso con el cumplimiento de las disposiciones previstas tanto en la citada LGPDPPSO como en los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos) por parte de todos los involucrados.

## **2. Alcance del documento**

Establecer los principales elementos que integran las medidas de seguridad administrativas, físicas y técnicas que ha adoptado la CNH para garantizar la confidencialidad, integridad y disponibilidad de los datos personales; así como determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto en un plano general los diversos sistemas de información y procesos en los se tratan datos personales por las diversas unidades administrativas, conforme a lo establecido en la LGPDPPSO y a los Lineamientos.

El alcance de este documento se relaciona con la identificación de sistemas de información o procesos administrados por parte de las Direcciones Generales y áreas adscritas a las distintas unidades de la CNH, en las que, de acuerdo con su ámbito de funciones, se llevan a cabo el uso y tratamiento de datos personales, mismos que se encuentran bajo su estricta responsabilidad tanto en los medios electrónicos como en los espacios físicos en que se administran, operan y resguardan los datos personales.

En este sentido, la Unidad de Transparencia integra el presente Documento de Seguridad con base en la información generada por las citadas unidades administrativas acorde al ámbito de sus funciones y de conformidad con las disposiciones jurídicas aplicables.

### 3. Glosario

**Análisis de brecha:** Concentración de elementos específicos que pueden existir entre lo deseable y lo actual.

**Análisis de riesgo:** Identificar peligros y estimar los riesgos, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento.

**Archivo:** Conjunto organizado de documentos producidos o recibidos por los sujetos obligados en el ejercicio de sus atribuciones y funciones, con independencia del soporte, espacio o lugar que

**Aviso de Privacidad:** 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 los mismos.

**Comité de Transparencia:** El Comité de Transparencia de la Comisión Nacional de Hidrocarburos.

**Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

**Datos personales sensibles:** Aquellos que se 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

**Derechos AR COP:** Los derechos de acceso, rectificación, cancelación,

**Ley General:** La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

**Lineamientos Generales:** Los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

**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

**Unidad Administrativa:** Las previstas en el Reglamento Interno de la Comisión Nacional de Hidrocarburos.

**Vulnerabilidad:** Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

**Vulneración de seguridad:** En cualquier fase del tratamiento de datos, al menos, las siguientes: I. La pérdida o destrucción no autorizada; II. El robo, extravío o copia no autorizada; III. El uso, acceso o tratamiento

## 4. Sistema de gestión de los datos personales

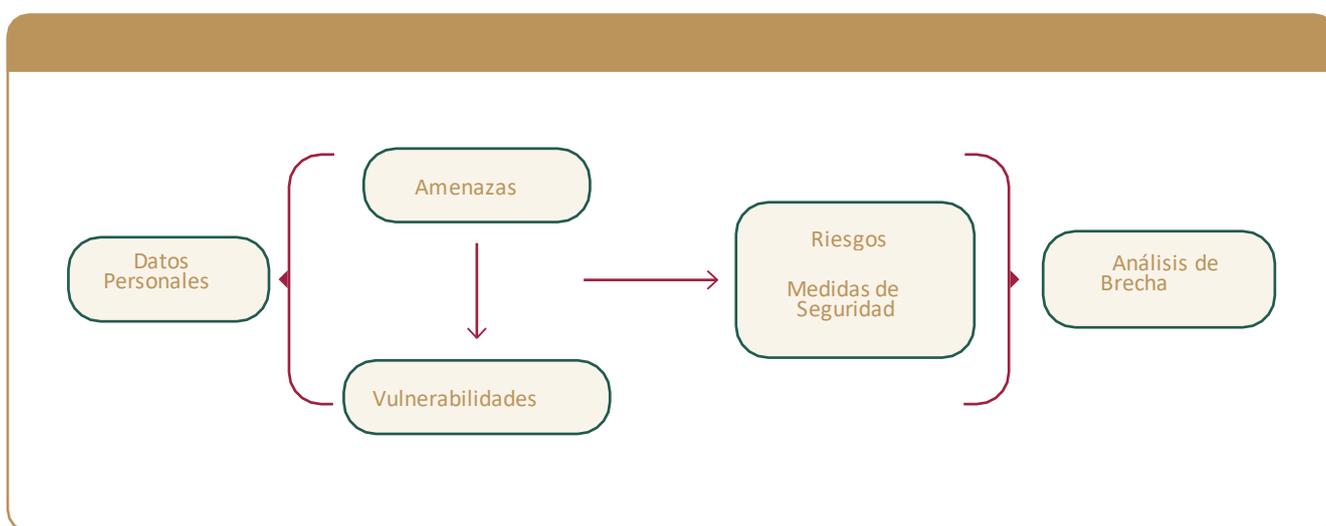
Para el tratamiento de los datos personales que lleva a cabo la CNH a través de su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismos, se realiza el establecimiento de políticas y métodos orientados a salvaguardar su confidencialidad, integridad y disponibilidad, conforme a los preceptos previstos por la LGPDPSO y la Ley General de Transparencia y Acceso a la Información Pública.

En tal virtud, la CNH tiene procesos, actividades y tareas en los que, de acuerdo con el ámbito de funciones de las distintas unidades administrativas que conforman la institución, se involucra el tratamiento de ese tipo de datos. Para ello, se dispuso de un formato que permitió a las diversas unidades administrativas realizar el levantamiento de inventarios de los datos personales que se encuentran bajo su responsabilidad, considerando los elementos mínimos que establece el artículo 33, fracción II, de la LGPDPSO y el diverso 58 de los Lineamientos.

Es así que a través del desarrollo de un instrumento homogéneo y estandarizado se llevó a cabo el levantamiento del inventario de datos, con el propósito de identificar, entre otros aspectos, la categoría y tipo de datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso a la operación sobre esos datos, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

De igual forma, una vez integrados los inventarios de datos (Anexo I), se realizó análisis de riesgos, en la cual, atendiendo a lo previsto en el artículo 33, fracción IV, de la LGPDPSO, las áreas responsables de su tratamiento identificaron los datos personales de acuerdo con su categoría; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para los titulares de los mismos con motivo de su posible vulneración y los factores de riesgo a los que eventualmente se encuentran expuestos.

Con base en dicho análisis de riesgo, además de promover el reconocimiento de las medidas de seguridad administrativas, entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; físicas, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento, así como técnicas que se valen de la tecnología para proteger el entorno digital de la información, el análisis de brecha a partir del cual será posible mitigar los riesgos a los que están expuestos los datos tratados, tal y como se ilustra a continuación en la siguiente imagen:



Considerando que la identificación de vulnerabilidades tiene por objeto prevenir posibles dificultades en la seguridad de los datos bajo un enfoque proactivo; es decir, identificar áreas de oportunidad en materia de seguridad de datos personales sin que éstas constituyan un daño efectivo, es que como posibles vulnerabilidades se listan las siguientes:

- Controles físicos y electrónicos inadecuados a sistemas de archivos.
- Deficiente conocimiento de procedimientos en materia de seguridad de datos.
- Inadecuada administración de autorizaciones de accesos a los datos personales (sistemas de privilegio).
- Falta de definición de perfiles y roles para delimitar funciones manejo y uso de datos.
- Falta de seguimiento y monitoreo a políticas de seguridad.
- Ausencia de mecanismos de confidencialidad por parte del personal (interno) o por terceros (externos).

Aunado a las anteriores vulnerabilidades, de manera enunciativa más no limitativa, se examinan algunos tipos de amenazas, que pueden ser intencionales o no, a las que podría enfrentarse la institución y sus activos de información.

Tipos de amenazas: Robo, extravío o copia no autorizada; uso, acceso o tratamiento no autorizado; daño, alteración o modificación no autorizado; pérdida o destrucción no autorizada y otras.

El riesgo que de manera general puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad por parte de las áreas comisionadas están orientadas a proteger los datos personales.

A partir de la identificación de vulnerabilidades y amenazas se han establecido medidas de seguridad generales que, de acuerdo a la experiencia y mejores prácticas, son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento. Como parte del sistema de gestión y política de seguridad institucional se enmarcan las reglas generales siguientes:

- Tratar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley General;
- Sujetar el tratamiento de los datos personales al principio de consentimiento, salvo las excepciones previstas por la Ley;
- Informar a los titulares del tratamiento de los datos y sus finalidades;
- Procurar que los datos personales tratados sean correctos y estén actualizados;
- Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron;
- Tratar los datos personales estrictamente para propósitos legales o legítimos;
- Limitar el tratamiento de los datos personales al cumplimiento de las finalidades;
- No obtener datos personales a través de medios fraudulentos;
- Respetar la expectativa razonable de privacidad del titular;
- Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades;

- Velar por el cumplimiento de los principios;
- Establecer y mantener medidas de seguridad;
- Guardar la confidencialidad de los datos personales;
- Identificar el flujo y ciclo de vida de los datos personales;
- Mantener actualizado el inventario de datos personales;
- Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales, y
- Identificar a los servidores públicos de la CNH responsables del tratamiento de los datos personales.

Con base en lo anterior, la CNH determina las pautas de acción del personal encargado de tratamiento de datos personales con miras a generar su correcto resguardo, buscando en todo momento actuar en apego a las directrices de la LGPDPSO y los Lineamientos Generales de la materia, siempre en consideración de la salvaguarda del derecho a la privacidad y protección de datos de las personas.

## 5. Inventario de Datos Personales

Para cumplir con los objetivos y obligaciones que prevé la LGPDPSO, particularmente en materia de seguridad y, como parte del Sistema de Gestión de Seguridad de Datos Personales de la CNH, se realizó una actualización dentro las unidades administrativas que conforman su estructura orgánica, para identificar los procesos en los que actualmente se lleva a cabo tratamiento de datos personales, obteniendo con ello el denominado Inventario de Datos Personales.

Por inventario de tratamiento de datos se entiende el control documentado del conjunto de operaciones que realizan las áreas que integran la CNH con motivo de los datos que se recaban de las personas, a través de procedimientos automatizados o físicos, que van desde su obtención, registro, organización, conservación, utilización, cesión, difusión, interconexión, hasta la rectificación, cancelación y oposición, con motivo de la atención del ejercicio de éstos derechos en el ámbito de sus atribuciones.

En tal virtud, en coordinación con las áreas y derivado del proceso de actualización de información, se advirtió que, en general 7 unidades administrativas, mismas que se encuentran integradas a su vez por direcciones generales, direcciones de área, subdirecciones, jefaturas de departamento y analistas, llevan a cabo el tratamiento de datos personales.

## Estructura Orgánica

|    |  |   |
|----|--|---|
| 1  | Dirección General de Dictámenes de Extracción                      | Aviso del Operador Petrolero a la Comisión Nacional de Hidrocarburos  |
| 2  | Dirección General de Dictámenes de Extracción                      | Informe Trimestral para seguimiento de los Programas de Aprovechamiento de Gas Natural Asociado   |
| 3  | Dirección General de Dictámenes de Extracción                      | Solicitudes del Operador Petrolero a la Comisión Nacional de Hidrocarburos Aprovechamiento de Gas   |
| 4  | Dirección General de Dictámenes de Extracción                      | Solicitud de aprobación de modificación al Plan de Desarrollo para la Extracción  |
| 5  | Dirección General de Dictámenes de Extracción                      | Solicitud de aprobación de la modificación del Programa de Trabajo y Presupuesto asociado a un Plan de Desarrollo para                      |
| 6  | Dirección General de Dictámenes de Extracción                      | Solicitud de aprobación del Plan de Desarrollo para la Extracción   |
| 7  | Dirección General de Dictámenes de Extracción                      | Aviso del Programa de Trabajo y Presupuesto de Planes de Desarrollo para la Extracción de Asignaciones                                      |
| 8  | Dirección General de Dictámenes de Extracción                      | Solicitud de aprobación del Programa de Trabajo y Presupuesto asociado a un Plan de Desarrollo para la                                      |
| 9  | Dirección General de Dictámenes de Extracción                      | Solicitud de aprobación del Plan de Programa de Transición  |
| 10 | Dirección General de Dictámenes de Extracción                      | Solicitud de aprobación o modificación del Programa Piloto referente a la producción temprana   |
| 11 | Dirección General de Dictámenes de Extracción                      | Aviso de Pozos que no requieren Autorización  |
| 12 | Dirección General de Dictámenes de Extracción                      | Aviso trimestral y de inicio de actividades relacionados con la Perforación de Pozos  |
| 13 | Dirección General de Dictámenes de Extracción                      | Notificaciones e Informes de actividades relacionadas con la Perforación de Pozos   |
| 14 | Dirección General de Dictámenes de Extracción                      | Informe de Indicadores de desempeño y de cumplimiento relacionados con la Autorización de Perforación de Pozos                              |
| 15 | Dirección General de Dictámenes de Extracción                      | Solicitud de Autorización de Perforación de Pozos   |
| 16 | Dirección General de Dictámenes de Extracción                      | Solicitud de Modificación de la Autorización de Pozos   |
| 17 | Dirección General de Dictámenes de Extracción                      | Solicitud de registro administrativo de Pozo  |
| 18 | Dirección General de Dictámenes de Extracción                      | Formato de Solicitud de Inscripción o Renovación al Padrón de Terceros Independientes en materia de Reservas                                |
| 19 | Dirección General de Recursos Humanos                              | Bolsa de Trabajo de la Comisión Nacional de Hidrocarburos   |
| 20 | Dirección General de Recursos Humanos                              | Expediente Personal de los Servidores Públicos de la Comisión Nacional de Hidrocarburos   |
| 21 | Dirección General Jurídica de Asignaciones y Contratos             | Sistema de Avisos de cambio de estructura de capital social de la Comisión Nacional de Hidrocarburos  |
| 22 | Dirección General Jurídica de Asignaciones y Contratos             | Sistema de Autorización para una Cesión de Control Corporativo y de Gestión de la Comisión Nacional de                                      |
| 23 | Dirección General Jurídica de Asignaciones y Contratos             | Sistema de Autorización para una Cesión de Control de las Operaciones de la Comisión Nacional de Hidrocarburos                              |
| 24 | Dirección General Jurídica de Asignaciones y Contratos             | Sistema de Avisos de cambio de cesión del Interés de Participación de la Comisión Nacional de   |
| 25 | Dirección General Jurídica de Asignaciones y Contratos             | Sistema de Solicitudes de reconocimiento de Caso Fortuito o Fuerza Mayor de los Contratos para la Exploración y Extracción de Hidrocarburos |
| 26 | Dirección General de Contratación para la Exploración y Extracción | Inscripción a las Licitaciones  |
| 27 | Dirección General de Autorización de Exploración                   | Formato ARES-A de solicitud de inscripción al Padrón ARES de la Comisión Nacional de Hidrocarburos  |
| 28 | Dirección General de Autorización de Exploración                   | Autorizaciones de Perforación de Pozos de la Comisión Nacional de Hidrocarburos   |

## 6. Análisis de riesgos y de brecha

El análisis de brecha de seguridad es un proceso que permite identificar las medidas de seguridad actuales y las que se necesitan para proteger los datos personales. Este análisis es fundamental para cualquier programa de protección de datos personales.

El análisis de brecha de seguridad se realiza a través de los siguientes pasos:

- Identificar la base de datos personales,
- Definir los objetivos del análisis
- Determinar el estado actual
- Identificar la brecha con respecto al estado deseado.

Una brecha de seguridad es un incidente que afecta a datos personales, ya sean tratados digitalmente o en papel. Este incidente puede ser accidental o intencionado, y permite que terceras personas accedan a datos que hasta entonces estaban protegidos.

## 7. Medidas de seguridad generales

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta la CNH para mantener la confidencialidad e integridad de la información, así como para proteger los datos personales contra daño, pérdida, destrucción o alteración; y evitar el uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada, son las siguientes:

### a) Medidas administrativas.

1. Adopción de un esquema de capacitación permanente en materia de la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados (LGPDPPO), impartido mediante el Campus Virtual de Capacitación del organismo garante.
2. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.
3. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes técnicos.
4. Mecanismos de control desarrollados conforme a lo establecido en los lineamientos del Sistema de Gestión de Documentos institucional.

5. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
6. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

#### **b) Medidas físicas.**

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.
2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.
3. Limitar el número de personas con acceso a archivos físicos.
4. Realizar el registro de personas con acceso a espacios físicos en los que se resguarda información con datos personales.
5. Procurar suscribir responsivas de confidencialidad con el personal que trata datos personales.
6. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.

#### **c) Medidas técnicas.**

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registradas a la vista de otras personas.
2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.
3. Notificar de manera inmediata a la Dirección General de Tecnologías de la Información en los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.
4. En la medida de lo posible utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.
5. Mantener los documentos electrónicos y físicos en lugares seguros, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.

6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.
7. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.
8. Borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que nos son necesarios para el desarrollo de funciones.
- 10.
9. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

## **8. Propuesta de capacitación en materia de datos personales**

Uno de los factores esenciales para la implementación de los controles y demás medidas de seguridad, la actualización y mejora continua del inventario de datos personales, el apego a la normatividad y a Ley, así como la concientización en la materia por parte del personal involucrado en el tratamiento de datos personales, es el conocimiento y capacitación, por lo que el aprovechamiento de los recursos y herramientas que el propio Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha dispuesto para su uso y obtención de beneficios, se propone que a través de los cursos se desarrolle un programa de capacitación focalizada, mediante el cual profundice en el conocimiento de la materia por parte de los servidores públicos que intervienen en el tratamiento de datos personales.

Así, entre los elementos de los que resulta necesario profundizar se encuentran los siguientes:

- Introducción al derecho a la protección de datos personales.
- Fundamentos conceptuales de la LGPDPSO
- La LGPDPPSO y sus Lineamientos.

## **9. Responsabilidades del tratamiento de datos personales**

1. Las unidades administrativas tendrán la obligación por disposición de ley, de eliminar la documentación y/o bases de datos en donde consten o se hagan constar datos personales que hayan dejado de ser necesarios conforme a las finalidades para las cuales se obtuvieron y haya concluido el plazo durante el cual se deben conservar.
2. Las unidades administrativas en atención a sus normas aplicables determinarán los medios de almacenamiento en los cuales se guardarán los datos personales que tratan, los cuales pueden ser físicos, electrónicos o mixtos.
3. Las unidades administrativas deberán tener debidamente identificadas a las personas que, en el ejercicio de sus funciones, puedan realizar tratamiento de datos personales, garantizando la restricción de acceso a terceros no autorizados.
4. Las personas que, con motivo de su empleo, cargo o comisión, tengan acceso a datos personales contenidos en medios electrónicos, deberán contar con contraseñas seguras las cuales no podrán ser compartidas con terceros.
5. Los datos personales contenidos en medios físicos deberán ser resguardados bajo llave, en espacios que garanticen su adecuada conservación.
6. Los papeles de oficina que contengan datos personales no podrán ser utilizados como papel de doble uso o de
7. Las personas que tengan acceso a datos personales, no podrán reproducirlos ni difundirlos mediante ningún medio sea físico o electrónico, a menos que sea necesario para el ejercicio de sus funciones.

8. La transferencia de datos personales que se realice a otros sujetos obligados del sector público podrá realizarse siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles y análogas con la finalidad que motivó el tratamiento.
9. Los datos personales en poder de la CNH, podrán ser utilizados para efectos estadísticos, garantizando la disociación de los
10. Los servidores públicos de la CNH que participen en el tratamiento de datos personales, deberán cumplir con la capacitación en materia de protección de datos personales que al efecto apruebe el Comité de Transparencia.
11. El personal de las unidades administrativas que trate datos personales deberá informar al Comité de Transparencia las vulneraciones de seguridad que se llegaran a presentar, así como reportar las acciones llevadas a cabo en consecuencia, a fin de que se informe a los titulares afectados para que puedan tomar las medidas correspondientes para la defensa de sus derechos.

Síguenos en nuestras Redes Sociales



@CNH\_MX



Comisión Nacional de Hidrocarburos



Comisión Nacional de Hidrocarburos



@cnh.mx