



DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES DEL CONOCER 2024

UNIDAD DE TRANSPARENCIA



ÍNDICE

Contenido

INTRODUCCIÓN.....	3
GLOSARIO.....	4
OBJETIVO.....	6
PARTE 1. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.....	7
PARTE 2. POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES O BUENAS PRÁCTICAS.....	10
PARTE 3. ANÁLISIS DE RIESGO.....	10
PARTE 4. ANÁLISIS DE BRECHA.....	11
PARTE 5. MEDIDAS DE SEGURIDAD A IMPLEMENTAR.....	12
PARTE 6. PROGRAMA GENERAL DE CAPACITACIÓN.....	14
PARTE 7. PLAN DE TRABAJO.....	16
PARTE 8. ACTUALIZACIONES.....	16



INTRODUCCIÓN

El presente Documento de seguridad se elabora de conformidad con lo establecido en el artículo 35¹ de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO) en el cual se establece la obligación del responsable de elaborar un documento de seguridad, que contenga el conjunto de acciones, actividades o mecanismos administrativos, técnicos y físicos, que permiten proteger los datos personales en posesión de sujetos obligados.

Las medidas de seguridad que adopte el responsable deberán considerar²:

- 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.

Las medidas de seguridad administrativas³ 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 físicas⁴ 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;

¹ Artículo 35 de la Ley General

² Artículo 32 de la Ley General.

³ Artículo 3, fracción XXI de la Ley General.

⁴ Artículo 3, fracción XXII, de la Ley General.



- 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 técnicas⁵ 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;
- 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.

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

⁵ Artículo 3, fracción XXIII, de la Ley General.



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;

OBJETIVO

El documento de seguridad, de conformidad con la Ley General⁶, 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.

Para dar cumplimiento a esta obligación, el presente documento de seguridad que contiene, lo siguiente⁷:

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

⁶ Artículo 3, fracción XIV, de la Ley General.

⁷ Artículo 35 de la Ley General.



- El análisis de brecha;
- 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 General⁸.

PARTE 1. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

1. A continuación se describen las categorías de datos personales con los que cuenta el CONOCER:

- **Datos de identificación y contacto:** nombre, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales.
- **Datos biométricos:** huella dactilar.
- **Datos laborales:** puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección y contratación y experiencia/capacitación laboral.
- **Datos académicos:** trayectoria educativa, título, cédula profesional, certificados y reconocimientos.
- **Datos patrimoniales y/o financieros:** ingresos, egresos y cuentas bancarias.
- **Datos legales:** situación jurídica de la persona [juicios, amparos, procesos administrativos, entre otros].
- **Datos de salud:** estado de salud físico presente, pasado o futuro.
- **Datos personales de naturaleza pública:** Datos que por mandato legal son de acceso público.

⁸ Artículo 33 de la Ley General



2. Personas de quienes se obtienen los datos personales:
 - a) Personas que laboran en el CONOCER.
 - b) Personas externas que prestan algún servicio para el CONOCER.
 - c) Personas externas que participan en actividades que llevan a cabo las direcciones del CONOCER [capacitaciones y cursos]. Los datos personales se recaban por medio de documentos presentados y/o por el llenado de formularios físicos y/o electrónicos por los titulares de los datos personales.
3. Las direcciones, subdirecciones y jefaturas encargadas de tratar datos personales son las siguientes:
 - Dirección General;
 - Coordinación de Promoción y Desarrollo;
 - Dirección de Gestión, Asesoría y Formación;
 - Dirección de Promoción y Desarrollo en los Sectores Productivos;
 - Dirección de Promoción y Desarrollo en los Sectores Social y de Gobierno;
 - Coordinación de Operación y Servicios a Usuarios;
 - Dirección de Promoción y Apoyo a Prestadores de Servicio;
 - Dirección de Acreditación y Certificación;
 - Dirección de Mercadeo, Comunicación y Canales de Atención;
 - Dirección de Administración;
 - Dirección de Planeación, Presupuesto y Finanzas;
 - Dirección de Asuntos Jurídicos; y
 - Órgano Interno de Control.



Las personas que desempeñan los puestos anteriormente mencionados, tienen como funciones y obligaciones las siguientes:

- a) Garantizar la seguridad en el tratamiento de datos personales, esto con la finalidad de evitar algún riesgo, como la pérdida, robo, alteración o acceso no autorizado.
 - b) Garantizar la debida protección de los datos personales, conforme a la Ley y las demás disposiciones aplicables en la materia.
 - c) Implementar medidas de seguridad físicas, técnicas y administrativas convenientes para el tratamiento diario de los datos personales.
 - d) Garantizar la confidencialidad de los datos personales derivada de los procedimientos que tienen a su cargo.
 - e) Conocer y aplicar las acciones derivadas de este Documento de Seguridad.
 - f) Garantizar el cumplimiento de los derechos ARCO a los titulares de los datos personales.
4. Nivel de seguridad de los datos personales a los que se les da tratamiento en el CONOCER: Para mayor garantía de seguridad en los datos personales y en las bases de datos personales, físicas o electrónicas, donde se concentran los mismos, las medidas de seguridad que se implementarán corresponden a un nivel de seguridad medio, siempre garantizando la confidencialidad, integridad y disponibilidad de los datos personales, tal y como lo expresa la Ley.
5. Transferencias de los datos personales: Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de la Ley General⁹.
6. Catálogo de bases de datos personales de las direcciones del CONOCER: Se anexa, al final de este documento, el catálogo de bases de datos personales con las que cuentan las direcciones del CONOCER, esto con la finalidad de que el titular de los datos personales conozca en donde se almacenan sus datos y más información relevante. Esto coadyuva al ejercicio de los derechos ARCO. [Anexo 1]¹⁰.

⁹ Artículo 22, 66 y 70 de la Ley General.

¹⁰ Catálogo de Bases de Datos Personales

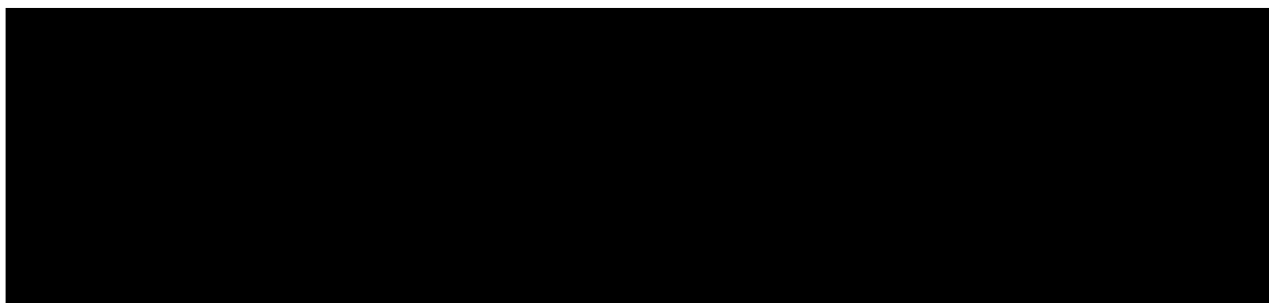
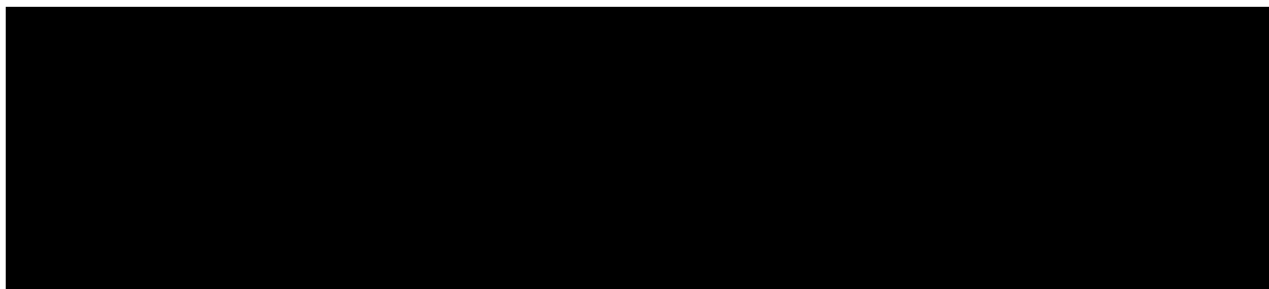


PARTE 2. POLÍTICAS INTERNAS PARA LA GESTIÓN Y TRATAMIENTO DE LOS DATOS PERSONALES O BUENAS PRÁCTICAS.

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.

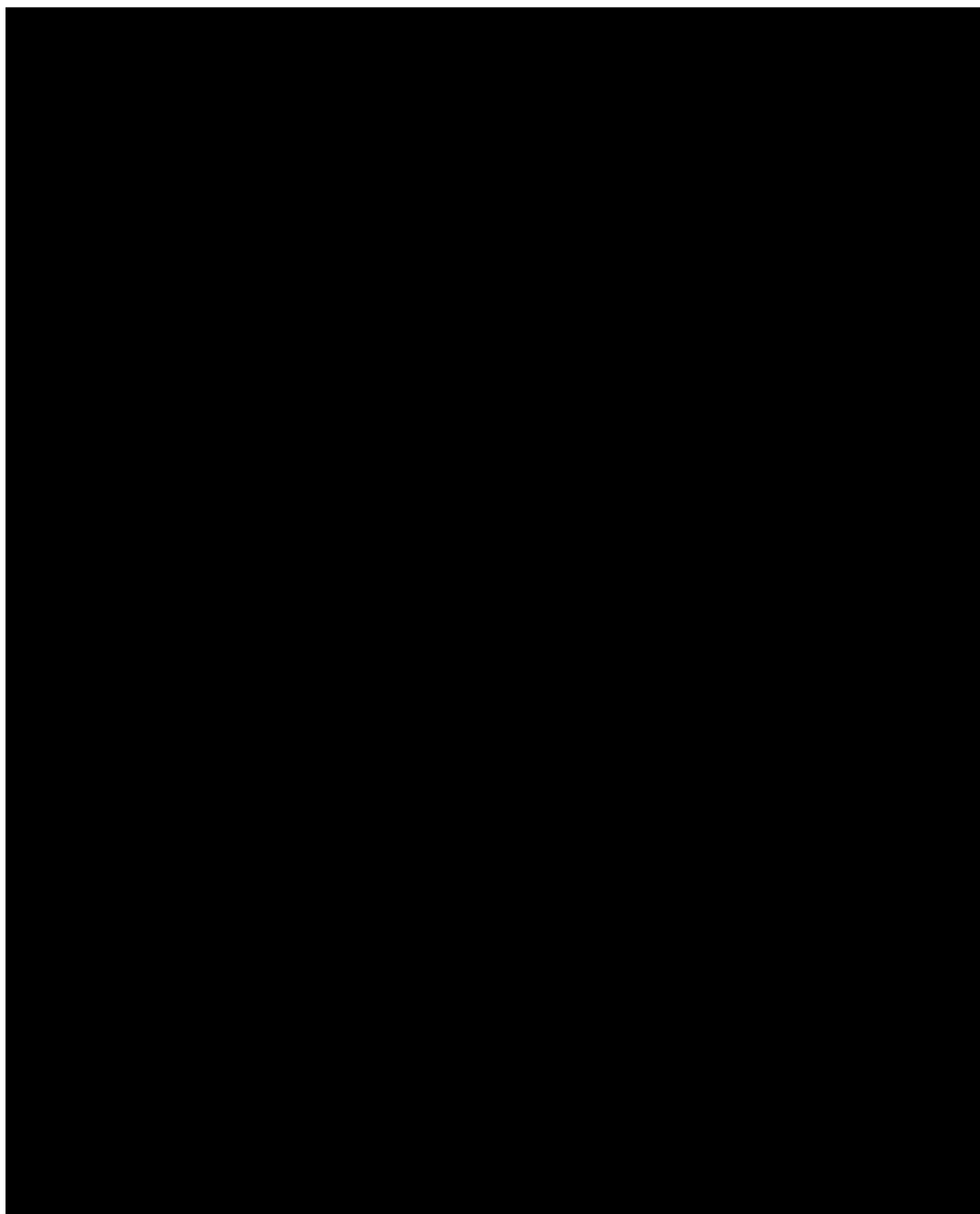
Debido a lo anterior y con fundamento en el artículo 30, fracción II, de la Ley General¹¹ en la materia, CONOCER como responsable de los datos personales que recaba y posee, ha desarrollado una Política de Protección de Datos Personales.

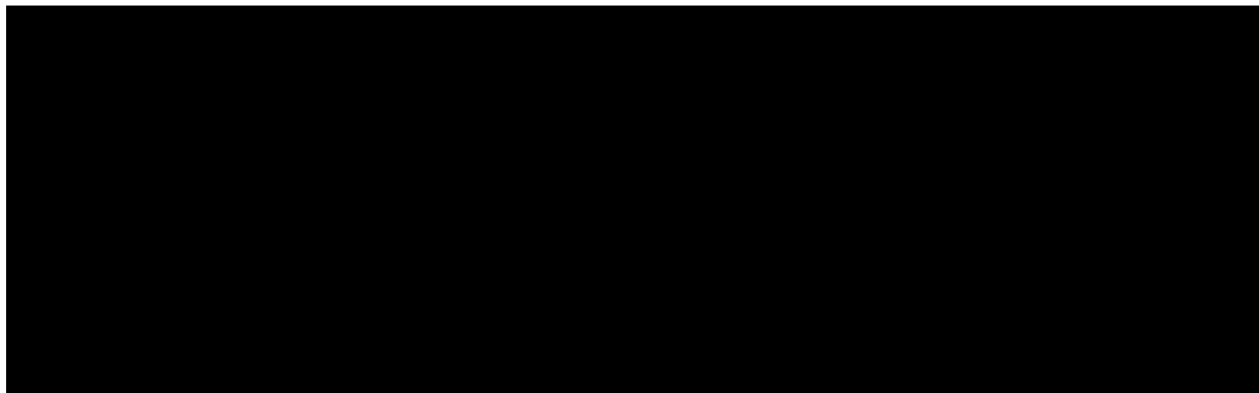
En general, todos los servidores públicos que laboran en el CONOCER que de forma manual o automatizada obtengan, usen, registren, organicen, conserven, elaboren, utilicen, comuniquen, difundan, almacenen, posean, accedan, manejen, aprovechen, transfieran o dispongan de los datos personales deberán de observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; de igual forma, siempre deberán de apegar su actuar a lo mandado 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 de conformidad con el documento de Política de protección de datos que elabore el CONOCER. [Anexo 2]¹².



¹¹ Artículo 30, fracción II de la Ley General.

¹² Política de Protección de Datos Personales del CONOCER.





PARTE 5. MEDIDAS DE SEGURIDAD A IMPLEMENTAR.

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales y que serán de aplicación a todas las bases de datos personales que manejan las personas a cargo de direcciones, subdirecciones y jefaturas mencionadas en el inciso 3. de la **Parte 1.** del presente documento, esto de acuerdo a sus funciones y obligaciones.

En ese sentido existen tres tipos de medidas de seguridad en el tratamiento de las bases de datos personales los cuales se definen a continuación:

- a) **Administrativos:** Medidas de seguridad basadas en la cultura del personal, conocidas como medidas de seguridad administrativas. Se encuentran enfocadas en roles y responsabilidades de personas o entidades involucradas en el tratamiento de datos personales.

La Ley define estas medidas como:

- 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.
- Sensibilización y capacitación del personal, en materia de Protección de Datos Personales.

Dentro de las medidas administrativas podríamos encontrar los siguientes ejemplos:

- Concientización del personal en seguridad de la información y Protección de Datos Personales.



- Políticas de escritorio limpio.
- Bloqueo de pantalla del equipo.
- Sanciones.

b) Técnicos: Medidas de seguridad en el entorno de trabajo digital, conocidas como medidas de seguridad técnicas. La Ley considera las acciones y mecanismos tecnológicos relacionados con software y hardware para proteger el entorno digital de datos personales y de los recursos involucrados en su tratamiento.

Para ello recomienda considerar al menos lo siguiente:

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea identificados y autorizados.
- Generar un esquema de privilegios para que el usuario realice las actividades que requiere con motivo de sus funciones.
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento de software y hardware.
- Gestionar de las comunicaciones, operaciones y medios de almacenamiento de los recursos informático en el tratamiento de datos personales.

Dentro de las medidas técnicas podríamos encontrar los siguientes ejemplos:

- Bloqueo de equipo por inactividad.
- Respaldos.
- Roles de usuario.
- Control de acceso.
- Desbloqueo de pantalla con contraseña.

c) Físicos: Medidas de seguridad en el entorno de trabajo físico, conocidas como medidas de seguridad físicas. La Ley de Datos considera la protección del



entorno físico de datos personales y de los recursos involucrados en su tratamiento y recomienda considerar lo siguiente¹³:

- Prevenir acceso no autorizado al perímetro, instalaciones físicas, áreas críticas, recursos e información.
- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas, recursos e información. La identificación, clasificación y borrado seguro de la 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;

En el caso del mantenimiento eficaz, busca asegurar en los equipos, la disponibilidad y la confidencialidad de datos personales, es decir, que siempre se pueda acceder a ellos y que sólo sean modificados por aquellos que han sido autorizados.

Dentro de las medidas físicas podríamos encontrar los siguientes ejemplos:

- Candados;
- Circuitos Cerrados de Televisión (CCTV);
- Bitácoras de entrada y salida de personal y visitantes.

PARTE 6. PROGRAMA GENERAL DE CAPACITACIÓN.

El programa de capacitación es una de las medidas de seguridad administrativa del tipo preventivo, efectiva y eficiente, en razón de que, permite que el tratamiento de datos personales se haga de una manera correcta y se evite el mal uso, sustracción, divulgación. Ocultamiento, alteración, mutilación, destrucción total o parcial y de manera indebida de datos personales, que pongan en peligro la confidencialidad, integridad y disponibilidad de la información.

¹³ Artículo 3, fracción XXII de la Ley General



El objetivo principal del programa de capacitación es capacitar y concientizar a las y los servidores públicos del CONOCER, en materia de protección de datos personales para el mejor desempeño de sus atribuciones, la especialización de sus funciones, el óptimo cumplimiento de los objetivos institucionales y promoción de la profesionalización en el servicio público.

Es de destacar que la capacitación en términos de protección de la información, permite a las personas identificar el tipo de información que manejan y el nivel de sensibilidad de la misma, además de conocer las mejores prácticas de tratamiento de la información desde el punto de vista de seguridad. Los planes de capacitación deben diseñarse e instrumentarse de acuerdo con el perfil y las responsabilidades de las personas a lo largo del ciclo de vida de los datos personales.

Resulta indispensable la obtención de técnica y perfeccionamiento de buenas prácticas en el tratamiento de los datos personales para el debido cumplimiento de las atribuciones de todo servidor público dentro del CONOCER.

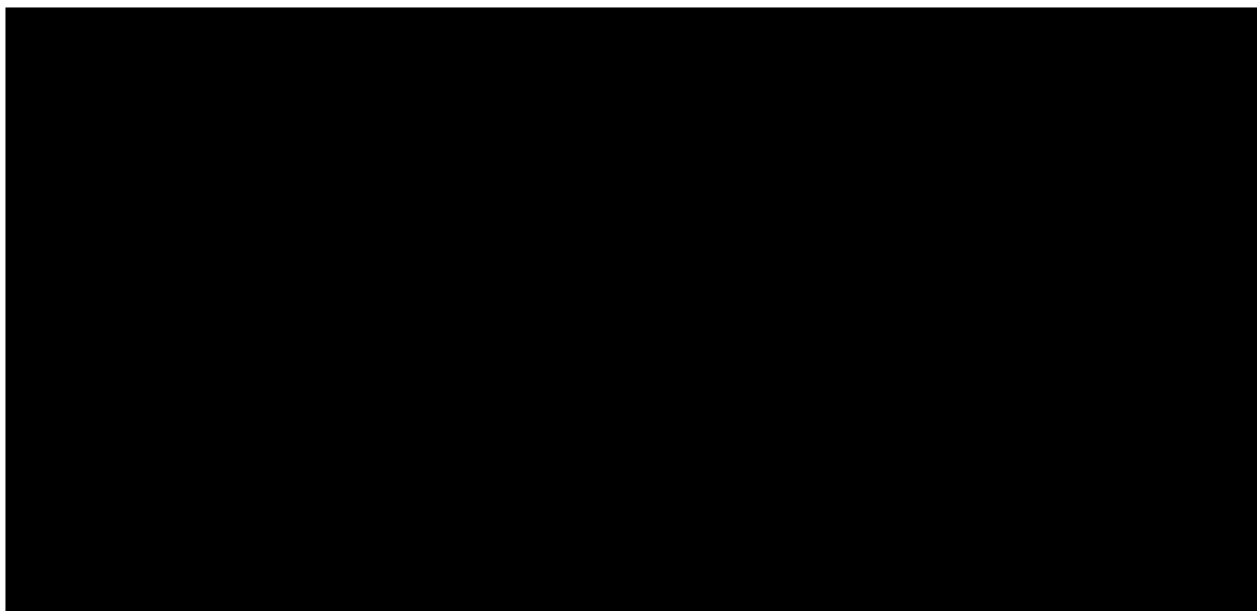
La parte de capacitación se considera una acción sumamente importante dentro del proceso de mejora continua.

Del mismo modo se busca garantizar la protección del tratamiento de los datos personales obtenidos como sujeto obligado, optimizar recursos, maximizar beneficios, establecer directrices para el correcto uso de la información en términos de su seguridad y generar esquemas de capacitación diferenciales e integrales que atiendan los siguientes rubros:

- Desarrollar los niveles de competencias laborales a través del perfeccionamiento de conocimientos, habilidades, actitudes y valores.
- Elevar los niveles de apropiación del conocimiento en materia de protección de datos personales.
- Establecer herramientas para realizar un efectivo tratamiento de datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición [ARCO].
- Garantizar la observancia de los principios de protección de datos personales previstos en la Ley General y demás disposiciones que resulten aplicables en la materia.
- Promover, fomentar y difundir una cultura de protección de datos personales.



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 en materia de protección de datos personales.



PARTE 8. ACTUALIZACIONES.

El presente documento de seguridad se actualizará cuando ocurran los siguientes eventos:

- I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad.
- IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
- V. Cuando surjan documentos, formatos, recomendaciones, etc. por parte del INAI para la mejora del documento de seguridad.

En todo lo relativo a este Documento de Seguridad de Protección de Datos Personales La Unidad de Transparencia asesorará a las Direcciones del CONOCER.



Anexo 1

Catálogo de Bases de Datos Personales

- **Datos identificativos:** El nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, demás análogos;
- **Datos electrónicos:** Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC [dirección Media Access Control o dirección de control de acceso al medio], así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet u otra red de comunicaciones electrónicas;
- **Datos Biométricos:** Huella Dactilar;
- **Datos laborales:** Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio y demás análogos;
- **Datos patrimoniales:** información fiscal, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales y demás análogos;
- **Datos sobre procedimientos administrativos:** La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio, demás análogos;
- **Datos académicos:** Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos y demás análogos.