SENER
SECRETARÍA DE ENERGÍA

CNSNS
COMISIÓN NACIONAL DE SEGURIDAD NUCLEAR Y SALVAGUARDIAS

POLÍTICAS DE SEGURIDAD EN LOS DATOS PERSONALES

COMISIÓN NACIONAL DE SEGUIRDAD NUCLEAR Y SALVAGUARDIAS (CNSNS)

Octubre 2022

2022 Año de Ricardo Flores Magón
PRECURSOR DE LA REVOLUCIÓN MEXICANA

ÍNDICE

I. INTRODUCCIÓN.

De acuerdo con los artículos 39, 40, 41, 42 y 43 del Reglamento Interior de la Secretaría de Energía, es un Órgano Administrativo Desconcentrado de la Secretaría de Energía, tiene por objeto Regular la seguridad nuclear, radiológica, física y las salvaguardias del uso pacífico de la energía nuclear para proteger la salud de la población y el ambiente.

Es así que, en apego a lo dispuesto por la Constitución Política de los Estados Unidos Mexicanos, en su artículo 6°, Base A, fracciones I y II, la información que posea la CNSNS es de máxima publicidad, pero la información concerniente a los datos personales será protegida en los términos y excepciones que fijen las leyes.

Derivado de lo anterior, es menester que en el CNSNS, se establezcan las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales y, que éstos atiendan a los principios de accesibilidad a la información, transparencia, objetividad e independencia con la correlación obligada de realizar acciones que coadyuven a identificar y adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal; que se extienda a las y los Responsables de la Administración de los Datos Personales y, en su caso, de las personas Encargadas del Tratamiento.

Por lo tanto, y en cumplimiento a lo que establecen los artículos 33 y 35, ambos de la LGDPPSO, y con el objeto de establecer y mantener las medidas de seguridad para la protección de los Sistemas de Datos Personales, las Unidades Administrativas de la CNSNS, deberán definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales; elaborar un inventario de Datos Personales; realizar un análisis de riesgos de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento; realizar un análisis de brecha; elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes; así como diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Es así que, se emite las presentes Políticas sobre el manejo de la Seguridad en los Datos Personales de la Comisión Nacional de Seguridad Nuclear y Salvaguardias, en apego a lo dispuesto por los artículos 33, 34, 35 y 36 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, cuya observancia es general y obligatoria para las Unidades Administrativas de la CNSNS y las personas servidoras públicas adscritas a las mismas, para establecer criterios, procedimientos institucionales y responsabilidades, a efecto de garantizar el derecho de acceso a la información pública que posee la CNSNS, de conformidad con la Ley General de Transparencia y Acceso a la Información Pública, Ley Federal de Transparencia y Acceso a la Información Pública, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás disposiciones legales y normativas aplicables.

Las presentes Políticas y sus anexos, son un instrumento necesario para establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Se adoptan tres niveles de seguridad basados en los estándares internacionales para la protección de datos personales[1], los cuales se aplicarán dependiendo del tipo de Datos Personales, tomando en cuenta los avances tecnológicos, la naturaleza de los datos almacenados y los riesgos a que estén expuestos.

II.- GLOSARIO.

1. Área de consulta de Datos Personales: El espacio destinado para que el personal autorizado examine aquellos datos personales que estén autorizados a consultar, sin posibilidad de modificar su contenido.
2. Área de recepción de Datos Personales: El espacio donde se reciben datos personales en cualquier tipo de soporte (físico, electrónico o ambos) en tanto se sigan las demás fases de su tratamiento para integrarlos a uno o más Sistemas de Datos Personales.
3. Área de resguardo de Datos Personales: El espacio para almacenar datos personales que han recibido el tratamiento correspondiente para que formen parte integral de uno o más Sistemas de Datos Personales, sin importar el soporte (físico, electrónico, o ambos) utilizado para su almacenamiento.
4. Base de datos personales: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
5. CNSNS: Comisión Nacional de Seguridad Nuclear y Salvaguardias.
6. Centro de Datos: Espacio físicos donde se concentran la Infraestructura Tecnológica principal y los Recursos de TIC necesarios para procesar, transmitir, almacenar, resguardar y respaldar la Información Electrónica institucional, es proporcionado por la Dirección Coordinadora de Tecnología, Reglamentación y Servicios (DCTRS) de la CNSNS.
7. 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.
8. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.
9. Divulgación de incidentes: Las acciones que adoptan el Titular del Área y el Responsable de los de Datos Personales, a efecto de dar a conocer a las Autoridades competentes, a los titulares de los datos y, en su caso, al público en general los actos deliberados (intrusión, robo, etc.), los acontecimientos de caso fortuito o de fuerza mayor (desastres naturales, incendios, huelgas, etc.) que hubieren ocasionado la pérdida total o parcial de los datos personales bajo su custodia.
10. 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.
11. Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

12. INAI o Instituto: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
13. LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
14. Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.
15. Plan de respaldo: Documento que refiere los tipos de respaldo de información y su periodicidad que se deben realizar para un Sistema informático desarrollado.
16. Responsable: Los sujetos obligados a que se refiere el artículo 1 de la LGDPPSO, que deciden sobre el tratamiento de datos personales, en el caso particular el CNSNS.
17. Soportes electrónicos: Medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, video y datos, fichas de microfilm, discos ópticos (CDs y DVDs.), discos magnético-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil.
18. Soportes físicos: Medios de almacenamiento inteligibles a simple vista, es decir que no requieran de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, formularios impresos llenados "a mano" o "a máquina", fotografías y placas radiológicas, entre otros.
19. Sistema informático: Conjunto de algoritmos y procedimientos que conforman aplicaciones o programas de cómputo que permiten procesar y almacenar datos bajo requerimientos definidos para cubrir alguna necesidad específica.
20. Sistemas de Datos Personales: Conjunto organizado de archivos, registros, documentos, bases o banco de datos personales en posesión de los sujetos obligados cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso.
21. SITE de Cómputo: Espacio físico con temperatura y humedad controlada, restringido y vigilado donde se encuentran los equipos de cómputo especializados y servidores, en la CNSNS.
22. Titular: La persona física a quien corresponden los datos personales.
23. Tratamiento de datos personales: 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
24. Unidades Administrativas: Todas aquellas unidades administrativas que se encuentran enlistadas en el Manual de Organización del CNSNS que tratan datos personales.
25. UT: Unidad de Transparencia de la CNSNS.

26. Zona de acceso restringido: Todas aquellas áreas a las que sólo tienen acceso el personal autorizado y el personal de vigilancia, es decir, el área de recepción, el área de resguardo y el área de consulta de datos personales.

III. MARCO JURÍDICO-ADMI

NISTRATIVO.

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Reglamento Interior de la Secretaría de Secretaría de Energía.
- Manual de Organización de la CNSNS
- Lineamientos Generales de Protección de Datos Personales para el Sector Público
- Lineamientos de Operación y Funcionamiento de Comité de Transparencia de la CNSNS
- Política Interna de Protección de Datos Personales del CNSNS
- Programa de Datos personales del CNSNS.

IV.OBJETO.

Las presentes Políticas tiene por objeto, acordar y divulgar los estándares, procedimientos y medidas de seguridad de carácter administrativos, físicos y técnicos, y los niveles de seguridad que se aplican para la seguridad de los Datos Personales en la CNSNS; así como los mecanismos y medidas de control que deberá emplear las personas servidoras públicas adscritas al CNSNS, responsable, los usuarios y encargados de los Datos Personales, de conformidad con las presentes Políticas y las normas establecidas para el efecto.

V. ÁMBITO DE APLICACIÓN.

El presente documento será de aplicación obligatoria para todas las personas servidoras públicas adscritas al CNSNS responsables de la administración y tratamiento de datos personales.

Así mismo, a las personas que deberán aplicar las políticas, estándares, procedimientos y controles de accesos administrativos, físicos y técnicos que se detallan en este documento:

a. Las personas responsables, de Datos Personales en el CNSNS;
b. El Comité de Transparencia del CNSNS, y
c. La Dirección Coordinadora de Tecnología, Reglamentación y Servicios de la CNSNS.

VI. DISPOSICIONES GENERALES.

A continuación, se integra de manera enunciativa las siguientes medidas que las áreas habrán de implementar en función del nivel de riesgo de cada uno de sus tratamientos:

MEDIDAS DE SEGURIDAD

Las medidas de seguridad de carácter administrativo son aquellas relacionadas con la organización del sujeto obligado. 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

6.1 MEDIDAS DE SEGURIDAD ADMINISTRATIVAS.

A. Declaración de confidencialidad: realizar esta declaración que será puesta a disposición del personal que interviene en el tratamiento de datos personales para que estén informados de los deberes y medidas de seguridad que deben tomar en consideración en sus actividades relacionadas con dichos tratamientos.

B. Listado de personal: elaborar un documento que contenga la relación del personal que interviene en el tratamiento de datos personales, en donde se incluya nombre, cargo, funciones en el tratamiento y obligaciones en materia de datos personales, por cada tratamiento.

C. Clasificación de los archivos físicos: identificar o incluir la base de datos en soporte físico en el Catálogo de Disposición Documental para tener control del ciclo de vida a que deben estar sujetos los archivos administrativos.

D. Clasificación de los archivos electrónicos: identificar y etiquetar las bases de datos en soporte electrónico con el nombre del Tratamiento de Datos Personales conforme al Inventario reportado por el área.

E. Capacitación: el personal involucrado en el tratamiento de los datos personales deberá asistir a los cursos de capacitación implementados por el Comité de Transparencia en el Programa Anual de Capacitación.

F. Bitácora de vulneraciones: implementar un control informativo en donde se reporten los tipos de vulneraciones[2] con los siguientes datos: fecha y lugar en donde se produjo, nombre y cargo de quien notifica la incidencia, nombre y cargo de la persona a la que se le comunica, y las medidas que se implementaron para subsanar la misma. Toda vulneración deberá notificarse, también, a la DCTRS para que tome las acciones pertinentes.

G. Si la vulneración trasciende a una posible afectación directa de los titulares de los datos personales, especialmente en sus derechos patrimoniales o en su esfera más íntima (datos sensibles), se deberá notificar a los titulares afectados para que tomen las medidas pertinentes para la defensa de sus derechos.

H. Depuración y borrado seguro del archivo físico: Transferir y depurar el archivo físico de manera periódica, conforme a los plazos de conservación y parámetros dispuestos la normativa en materia.

I. Depuración y borrado seguro del archivo electrónico: borrar, de manera segura y permanente, las bases de datos o parte de ellas que se encuentren en archivo electrónico, en desuso o que hayan cumplido su finalidad o el tiempo de conservación dispuesto para el archivo administrativo. Solicitar a la Dirección Coordinadora de Tecnología, Reglamentación y Servicios de la CNSNS que proporcione un programa para el borrado de la información, o en su defecto, reinicio de los equipos o medios de almacenamiento a los valores de origen. Además, para la depuración y borrado seguro de las bases de datos electrónicas, se deberá levantar un acta, signada por el titular del área y remitirse copia de la misma a la UT.

J. Bitácora de consulta: establecer una bitácora como control para registrar el nombre, cargo, fecha y hora de consulta de la base de datos.

K. Responsable de seguridad: designar un responsable de seguridad para coordinar y verificar las medidas de seguridad establecidas en el Documento de Seguridad.

L. Transferencias: realizar transferencias con las medidas de confidencialidad necesarias, enviar la información en sobre cerrado y con la leyenda de "confidencial" o en archivos electrónicos encriptados.

Las medidas de seguridad de carácter físico son aquellas encaminadas a la protección del entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Algunas medidas previstas por la propia LGPDPPSO son las de prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información; proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; entre otros.

La CNSNS cuenta con el apoyo de la Subdirección de Servicios Generales, misma que se ocupa de brindar y supervisar los servicios de seguridad a las personas servidoras públicas adscritas a la CNSNS dentro de las instalaciones, así como de preservar los bienes muebles e inmuebles de la misma; establecer, coordinar y mantener un sistema riguroso para el control de los ingresos y de acceso para el control y registro de la identificación oficial de las personas servidoras públicos y usuarios; vigilar e inspeccionar de forma sistemática para fines de seguridad.

6.2 MEDIDAS DE SEGURIDAD FÍSICAS

A. Cuidado de los bienes informáticos: Mantener en buen estado el bien informático que le haya sido asignado y no abrir los equipos o bien, introducir en ellos cualquier tipo de instrumento o software que no sean los apropiados para el trabajo y que no hayan sido validados por la DIC, tampoco alterar el orden de los cables conectados[3].

B. Prevenir accesos no autorizados: prevenir que el acceso a las bases de datos o a la información, así como a los recursos que las contengan, se realice únicamente por usuarios identificados autorizados por el área.

C. No instalar equipos ajenos: Abstenerse de instalar equipos de cómputo que no sean propiedad del CNSNS sin permiso del área administrativa correspondiente y de la DIC. Los usuarios que requieran hacer uso de la red interna del CNSNS deben usar solamente las direcciones IP asignadas por la

DIC En caso de requerir conectar un dispositivo de almacenamiento de información (p. ej. USB, disco duro portátil, etcétera) al equipo del usuario, éste debe ser revisado previamente por el antivirus. En el caso de encontrarse infectado el dispositivo, el usuario debe extraer inmediatamente sin consultar, modificar o copiar información alguna.

D. Traslado de equipos de cómputo: En su caso se deberá observar lo dispuesto por la Coordinación de Servicios Tecnológicos, para el traslado de equipos de cómputo fuera de las instalaciones del CNSNS.

E. Archivero con candado: Resguardar las bases de datos en archivo físico en un archivero con candado o con llave de seguridad, cuyo acceso sólo será permitido al personal autorizado.

F. Zona de confidencialidad: definir una zona de confidencialidad en donde se resguardarán los archivos físicos o equipos de cómputo que contengan las bases de datos, cuya finalidad sea limitar el acceso al personal no autorizado, equipos o aparatos de copiado. Para el caso de los equipos de cómputo se dispondrá del Centro de Datos y del SITE de Cómputo.

Por último, las medidas de seguridad de carácter técnico son el conjunto de acciones y mecanismos que se valen de la tecnología relacionada con el hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. Algunas medidas establecidas en la LGPDPPSO son las de prevenir 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; gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales, entre otras.

Sobre este tipo de medidas, la CNSNS a través de la Dirección Coordinadora de Tecnologías, Reglamentación y Servicios (DCTRS) como enlace informático, entre otras labores la administración de los recursos en materia de tecnologías de la información y comunicación y proveer los servicios que se requieran en la materia; planear, diseñar, mantener y supervisar la operación de los sistemas de información y comunicación que requieran los órganos y áreas; proporcionar los servicios de mantenimiento a las redes, sistemas, equipo informático, comunicación y digitalización de las áreas que integran el CNSNS y; ejecutar y actualizar los mecanismos de seguridad informática y vigilar su adecuado funcionamiento.

6.3 MEDIDAS DE SEGURIDAD TÉCNICAS

A. Cuidado de la contraseña personal: abstenerse de compartir contraseñas personales de la red institucional, las contraseñas, tokens, identificadores o cualquier mecanismo utilizado para la autenticación en un recurso informático del CNSNS

B. Actualización de contraseñas: Se realizará cada año cuando menos debido a que los equipos de cómputo de la CNSNS, la Dirección Coordinadora de Tecnología, Reglamentación y Servicios (DCTRS) realiza el cambio a través de su sistema de control.

C. Reportar fallas: notificar al área correspondiente cualquier fallo, error, sospecha, violación o incumplimiento a las políticas de seguridad de la información.

D. No instalar softwares: abstenerse de descargar en el equipo de cómputo institucional software y aplicaciones de lugares no seguros o dudosa procedencia.

E. Contraseñas robustas: se sugiere construir contraseñas con rol de administrador de forma robusta, atendiendo a los siguientes criterios:

- Contar con una longitud mínima de 12 caracteres.
- Incluir, por lo menos, dos letras mayúsculas, dos letras minúsculas, dos símbolos especiales (punto, coma, guion, etcétera) y un número;
- Evitar el uso de palabras comunes o datos personales;
- Renovarlas de manera periódica;
- Las contraseñas no podrán repetirse en al menos 10 interacciones;
- Almacenarlas de forma cifrada y en archivos electrónicos distintos en los que se almacenan datos de aplicaciones.

F. Respaldo de información: realizar respaldos de la información que resida en el equipo de cómputo asignado está es responsabilidad del usuario del equipo de cómputo, el cual deberá contar con el equipo de almacenamiento, autorización de su unidad administrativa correspondiente y la DIC brindará la asesoría

NIVELES DE SEGURIDAD.

Los niveles de seguridad, se identificarán por cada Responsable de la Administración de los Datos Personales, considerando los estándares Internacionales de Seguridad Aplicables y las Recomendaciones sobre medidas de seguridad aplicables a los Sistemas de Datos Personales.

Los niveles de seguridad responden a la mayor o menor necesidad de garantizar la integridad de los datos personales. Por lo tanto, las Unidades Administrativas y sus Responsables aplicarán el nivel básico, medio o alto de medidas de seguridad.

Aunado a lo anterior, para determinar el nivel de riesgo se considera el criterio del riesgo inherente del dato personal, así como el nivel se seguridad requerido para éste, en adición a las vulnerabilidades y amenazas, de acuerdo con las categorías o tipos de datos personales que se detallan a continuación:

	CRITERIOS DEL NIVEL DE RIESGO	
A	Riesgo Inherente Básico	Nivel de Seguridad Básico
B	Riesgo Inherente Medio	Nivel de Seguridad Medio
C	Riesgo Inherente Alto	Nivel de Seguridad Alto

A.- NIVEL BÁSICO

Las medidas de seguridad de NIVEL BÁSICO serán aplicables para los Datos Personales que enseguida se mencionan:

a.1. IDENTIFICACIÓN: Nombre, domicilio, correo electrónico, número de teléfono; RFC, CURP, cartilla militar, estado civil, firma, firma electrónica, lugar de nacimiento, fecha de nacimiento, nacionalidad, edad, nombres de familiares, dependientes, beneficiarios, fotografía, idioma o lengua, entre otros.

B. NIVEL MEDIO

Los Datos Personales que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico, deberán observar las marcadas con nivel medio.

b.1. DATOS PATRIMONIALES: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales, entre otros.

b.2. DATOS SOBRE PROCEDIMIENTOS ADMINISTRATIVOS SEGUIDOS EN FORMA DE JUICIO Y/O JURISDICCIONALES: Información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

b.3. DATOS ACADÉMICOS: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.

b.4. DATOS DE TRÁNSITO Y MOVIMIENTOS MIGRATORIOS: Información relativa al tránsito de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

C. NIVEL ALTO

Los Datos Personales que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico y medio, deberán tomar las marcadas con nivel alto.

c.1. DATOS IDEOLÓGICOS: Creencia religiosa, ideológica, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.

c.2. DATOS DE SALUD: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.

c.3. CARACTERÍSTICAS PERSONALES: Tipo de sangre, ADN, huella digital, u otros análogos.

c.4. CARACTERÍSTICAS FÍSICAS: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.

c.5. VIDA SEXUAL: Preferencia sexual, hábitos sexuales, entre otros.

c.6. ORIGEN: Étnico o racial.

VII.-ESPECIFICACIONES TÉCNICAS.

7.1 INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, las Unidades Administrativas del CENAPRED deberán elaborar un Inventario de los Sistemas de Datos Personales y su Tratamiento (ANEXO 1).

INVENTARIO DE DATOS PERSONALES Y SU TRATAMIENTO (ANEXO 1)							
Unidad administrativa	Nombre del Sistema	Responsable del Sistema		Tipo de Datos Personales contenidos en el Sistema	Nivel de Seguridad	Uso que se le da al Sistema	Objeto del Sistema
		Nombre	Cargo				

7.2 FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATO PERSONALES.

Para establecer y mantener las medidas de seguridad para la protección de los Sistema Datos Personales, las Unidades Administrativas del CNSNS, deberán definir las funcione y obligaciones del personal involucrado en el tratamiento de los datos personales. (ANEXO 2).

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Anexo 2) Arts. 33, fracc. II y 35, fracc. II de la LGPDPPSO						
Artículo 35, Fracción II...						
II. Las funciones y obligaciones de las personas que traten datos personales; Objetivo: Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;						
	Unidad Administrativa	Responsable del Sistema	Cargo	Nombre del Sistema de Tratamiento de Datos Personales	Funciones	Obligaciones
1						

Nivelación de las medidas de seguridad de acuerdo con el nivel de riesgo.

Las medidas de seguridad que deberán adoptarse deben tomar como referencia el nivel de riesgo latente que presenta cada tratamiento de datos personales.

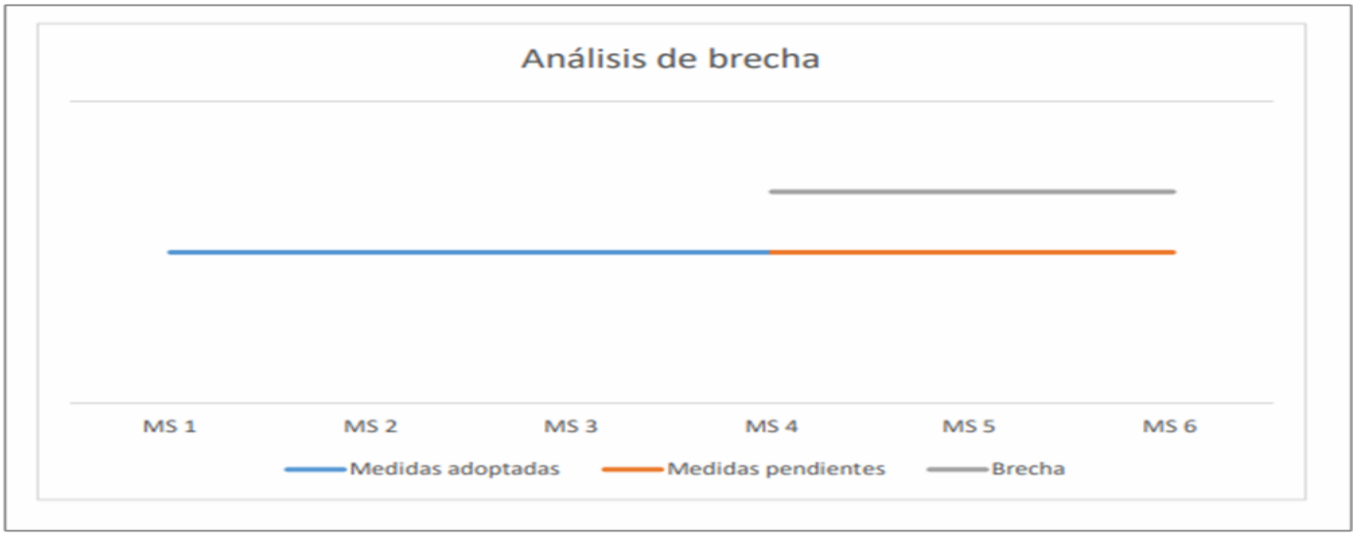
7.3 MATRIZ DE RIESGOS Y ANÁLISIS DE BRECHA.

Con el objeto de establecer y mantener las medidas de seguridad para la protección de los Datos Personales, las Unidades Administrativas del CNSNS deberán realizar un análisis de riesgo de los datos personales, y un análisis de brecha comparando las medidas de seguridad existentes contra las faltantes de cada uno de los oficios, archivos o documentos que contengan Datos Personales; considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.

7.3.1 ANÁLISIS DE BRECHA

El análisis de brecha consiste en identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados.

Por ejemplo, si se recomienda implementar al tratamiento “A” un conjunto de medidas “C”, y el área responsable de dicho tratamiento informa que de ese conjunto de medidas hacen falta implementar algunas, la identificación de lo que hace falta implementar se conoce como brecha.



El análisis de brecha es de naturaleza diagnóstica y contribuye a conocer las áreas de oportunidad por cada tratamiento.

A continuación, se presenta el Formato de Matriz de Riesgos y Análisis de Brecha que deberán requisitar todas las Unidades Administrativas que mantienen y operan Sistemas de Datos Personales. (ANEXO 3).

MATRIZ DE ADMINISTRACIÓN RIESGOS

UNIDAD ADMINISTRATIVA:

Nombre del Proceso: PROTECCIÓN DE DATOS PERSONALES / INFORMACIÓN DIGITAL

ANÁLISLS DE RIESGOS					**EVALUACIÓN DE RIESGOS**			**ANÁLISIS DE BRECHA**		
Unidad Administrativa	Ubicación de la Información Físico o digital	Tipo de Dato Personal	Nivel de seguridad	Riesgo	Posibilidad de Ocurrencia	Impacto	Nivel de Riesgo	Respuesta al Riesgo	Establecimiento de Actividades de Control	
									Preventivas/ Responsable	Correctivas/ Responsable

7.4 PLAN DE TRABAJO.

Formato del Plan de Trabajo que deberán requisitar todas las Unidades Administrativas que mantienen y operan Sistemas de Datos Personales. (Anexo 4).

Conforme al análisis de brecha, existen algunas medidas de seguridad que se requieren y que aún no han sido definidas e implementadas, por lo que a continuación se presentan las actividades que se planean llevar a cabo para cada una de estas:

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Anexo 4) Arts. 33, fracc. VI y 35, fracc. V de la LGPDPPSO.	
Plan de Trabajo	
Medidas de seguridad faltantes	Actividades por desarrollar

7.5 MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

En cumplimiento a lo que establecen los artículos 33, fracción VII y 35, fracción VI de la LGDPPSO, se deberán monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

En éste contexto, es importante señalar la diferencia entre un soporte físico y un soporte electrónico.

- Soportes electrónicos: Medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, discos ópticos (CDs y DVDs.), discos magnético-ópticos, discos magnéticos (flexibles y duros) y demás mediosde almacenamiento masivo no volátil.

- Soportes físicos: Medios de almacenamiento inteligibles a simple vista, es decir, que no requieran de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, formularios impresos llenados "a mano" o "a máquina", fotografías y placas radiológicas, entre otros.

Con independencia del tipo de sistema en el que se encuentren los Datos Personales o el tipo de tratamiento que se efectúe, el personal titular de la Unidad Administrativa responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico; en estas últimas, podrá solicitar para tal efecto el apoyo de la Dirección de Instrumentación y Cómputo para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, debiendo solicitar para ello la intervención de la Coordinación de Servicios Tecnológicos de la SSPC en ejercicio de las atribuciones que le confiere al Manual de Organización Específico de la SSPC

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales que implementen las Unidades y Áreas Administrativas responsables de Sistemas de Datos Personales deberán estar documentadas y contenidas en el Sistema de que se trate, en términos de lo dispuesto por la LGDPPSO.

7.6.1 POLÍTICAS DE APLICACIÓN DE NIVEL BÁSICO DE SEGURIDAD PARA LOS SISTEMAS DE DATOS PERSONALES.

7.6.2 ACCESO Y CONSULTA DE DATOS PERSONALES.

El personal responsable de los Sistemas de Datos Personales, mantendrá un estricto control y registro de las autorizaciones emitidas para facultar al personal del CNSNS, o personal externo encargados del tratamiento de datos personales.

- El acceso a los Datos Personales, sólo se proporcionará al personal del CNSNS y personal externo que, por razón de su empleo, cargo o comisión, tengan la necesidad de acceder a éstos para el desarrollo de las actividades institucionales.

- Deberá darse a conocer al personal del CNSNS y personal externo a los que se les proporcione el acceso a los Sistemas de Datos Personales, las

situaciones que son consideradas como uso inadecuado, así como de las consecuencias de incurrir en alguna de ellas.

- Deberán establecerse medidas de control de acceso físico y lógico para reducir la probabilidad de que los Datos Personales sean accedidos por personal no autorizado, dichos controles deberán cumplir con los requisitos de seguridad propios del tipo de información, así como de los requerimientos legales y administrativos correspondientes.
- Las autorizaciones al personal del CNSNS y personal externo que por razón de su empleo, cargo o comisión tengan la necesidad de acceder a los Datos Personales, que solicitan permiso para introducir a las zonas de acceso restringido aparatos como computadoras, monitores, pantallas planas, laptop o agendas electrónicas, el encargado debe registrar:
  - Nombre del solicitante;
  - Nombre del equipo a introducir;
  - Fecha y hora de la introducción;
  - Razón de la introducción y tiempo que se quedará;

7.6.3 DIVULGACIÓN DE INCIDENTES.

En caso de que ocurra una vulneración de seguridad, el personal responsable deberá analizar las causas por las cuales se presentó e implementará en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

Se considerarán como vulneraciones 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 no autorizado, o

IV. El daño, la alteración o modificación no autorizada.

El personal responsable deberá llevar una bitácora de las vulneraciones de seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

El personal responsable deberá informar por los medios de comunicación más inmediatos y sin dilación alguna al titular de los datos personales, y según corresponda, al INAI, las vulneraciones de seguridad que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

El personal responsable deberá informar al titular de los datos personales al menos lo siguiente: I. La naturaleza del incidente;

II. Los datos personales comprometidos;

III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;

IV. Las acciones correctivas realizadas de forma inmediata, y

V. Los medios donde puede obtener más información al respecto.

En caso de robo o extravío de datos personales en soportes físicos y/o electrónicos, el personal responsable de los Sistemas de Datos Personales que corresponda, al tener conocimiento del incidente, dará vista al Órgano Interno de Control y a la Coordinación Administrativa para que en uso de facultades presenten en sus respectivas competencias, denuncia o querella en términos del Reglamento Interior de la Secretaría de Seguridad y Protección Ciudadana haciéndolo del conocimiento de la Unidad de Transparencia, para que de acuerdo a sus atribuciones determinen lo conducente.

El personal responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

7.6.5.
SUPERVISIÓN.

De conformidad a lo establecido en el artículo 84, fracción V de la LGDPPSO, el Comité de Transparencia habilitará a personal de la Unidad de Transparencia para realizar periódicamente una supervisión conjunta con la Dirección de Instrumentación y Cómputo que coadyuva a proteger desde el ámbito tecnológico la información electrónica institucional, los recursos informáticos y los servicios tecnológicos necesarios para que el CNSNS pueda cumplir con las funciones y obligaciones que le corresponda de acuerdo a la normatividad aplicable, así como con las Unidades Administrativas que manejan Datos Personales, para el cumplimiento de las medidas, controles y acciones previstas en el presente documento, ello independientemente de las medidas adoptadas por el INAI.

7.6.6. CANCELACIÓN DE DATOS PERSONALES.

Para proceder a la baja o destrucción documental de soportes físicos que contienen datos personales, se observarán las disposiciones en materia de archivos que emita la CNSNS.

Todo soporte electrónico que sea dado de baja (ya sea por obsoleto, sustitución, ejercicio del derecho de cancelación o alguna otra causa) deberá pasar por un proceso de preparación final antes de ser desechado. Dicho proceso incluye; la transferencia del contenido que es preciso conservar hacia otro soporte electrónico y la destrucción, inhabilitación o daño que deje inservible dicho soporte.

El personal encargado de los Datos Personales, vigilará que se sigan los procedimientos y se utilicen los mecanismos para asegurar la destrucción de soportes electrónicos que contengan datos personales.

El personal encargado llevará una bitácora donde registrará la baja de soportes electrónicos que contienen datos personales la cual deberá contener:

I. Nombre y firma de la persona que realiza la acción;

II. Fecha y hora que se realiza;

III. El destino que se le dará al soporte electrónico desechado;

IV. Nombre y firma del responsable y del Titular del Área Administrativa correspondiente.

7.6.7. SOPORTES FÍSICOS

El CENAPRED en la medida de su disponibilidad presupuestaria y de recursos humanos, físicos y materiales, apoyarán los programas y acciones que se implementen para el cumplimiento de las políticas de seguridad objeto del presente instrumento para el desarrollo de los siguientes apartados.

A.- ÁREA DE RECEPCIÓN DE DATOS PERSONALES.

- Deberá existir la infraestructura apropiada, mantener en forma organizada y segura los datos personales recibidos en dicha área de recepción y se deberán seguir los procedimientos establecidos para el efecto.
- La recepción de datos personales deberá realizarse en las oficinas de los servidores públicos, cuyas funciones tengan a cargo dicha recepción.
- Al momento de la recepción deberá informarse al titular de los datos personales el objetivo de su recolección.
- El expediente confidencial deberá resguardarse en el mobiliario identificado, bajo llave, dentro de la oficina del director de área responsable de su resguardo.
- El personal autorizado para la recepción deberá ostentar una identificación visible con fotografía (credencial o Gafete) emitida por el CNSNS.
- El personal responsable de los Sistemas de Datos Personales debe actualizar periódicamente los nombres completos y fotografías que se deben exhibir en lugar visible dentro y fuera del área de recepción de datos personales, conforme se vayan presentando cambios de personal.
- No está permitido el libre acceso de personal no autorizado ni de equipo dentro del área de recepción a menos que sea autorizado por el personal Responsable.
- Debe existir señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de recepción.

B.- ÁREA DE RESGUARDO DE DATOS PERSONALES.

- Debe existir la infraestructura apropiada, mantener en forma organizada y segura los datos personales recibidos en dicha área de resguardo en soportes físicos y/o electrónicos.
  - De existir ventanas o muros transparentes en el área de resguardo, la visión deberá estar obstruida con material que impida la observación de los datos personales.
- Deben existir las condiciones ambientales idóneas para preservar el estado físico de los documentos que contienen los datos personales durante el tiempo de la conservación.
- La puerta de acceso al área de resguardo debe contar con cerradura, dispositivo

electrónico o cualquier tecnología que impida su libre apertura, este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área.

- El mobiliario utilizado dentro del área de resguardo protegerá los datos personales en soportes físicos de condiciones adversas en humedad, temperatura, iluminación solar, polvo, consumo de alimentos y presencia de plagas entre otras.
- El personal autorizado para el área de resguardo, deberá ostentar una identificación visible con fotografía (credencial o Gafete) emitida por el CNSNS.
- El personal responsable de los Sistemas de Datos Personales debe actualizar periódicamente los nombres completos y fotografías que se deben exhibir en lugar visible dentro y fuera del área de resguardo de datos personales, conforme se vayan presentando cambios de personal.
- No está permitido el libre acceso de personal no autorizado ni de equipo dentro del área de resguardo.
- Debe existir señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de resguardo.

C.- ÁREA DE CONSULTA DE DATOS PERSONALES.

- Debe existir la infraestructura apropiada y seguir los procesos y procedimientos necesarios de tal manera que sea posible supervisar y vigilar los datos personales en soportes físicos que consultan os responsables de los datos dentro del área de consulta.
- De existir ventanas o muros transparentes en el área de consulta, la visión deberá estar obstruida con material que impida la observación de los datos personales.
- La puerta de acceso al área de consulta debe contar con cerradura, dispositivo electrónico o cualquier tecnología que impida su libre apertura, este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área.

- El personal autorizado para el área de consulta, deberá ostentar una identificación visible con fotografía (credencial o Gafete) emitida por el CNSNS.
- El personal del área de consulta debe actualizar periódicamente los nombres completos y fotografías que se deben exhibir en lugar visible dentro y fuera del área de consulta de datos personales, conforme se vayan presentando cambios de personal.
- No está permitido el libre acceso de personal no autorizado ni de equipo dentro del área de consulta, a menos que lo autorice el responsable.
- Debe existir señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de consulta.
- La Coordinación Administrativa del CNSNS será la encargada de hacer de conocimiento al personal operativo de limpieza de las restricciones de acceso y las prohibiciones.
- Cuando la persona titular de los datos personales requiera el acceso a los mismos, se procederá conforme al procedimiento establecido en el Titulo Tercero de la LGDPPSO.

7.6.8. SOPORTES ELECTRÓNICOS.

A.- ÁREA DE RECEPCIÓN DE DATOS PERSONALES.

- El equipo de cómputo instalado en el área de recepción debe cumplir con los niveles de seguridad para ser ocupada en zonas de acceso restringido y con el software autorizado por la Coordinación De Servicios Tecnológicos de la SSPC.
- El equipo de cómputo deberá estar provisto de la tecnología necesaria y suficiente para verificar la identidad del personal autorizado que labora en el área de recepción. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda a la recepción de datos personales.

B.- ÁREA DE RESGUARDO DE DATOS PERSONALES.

- El equipo de cómputo cumple con la tecnología necesaria y suficiente para verificar la identidad del personal autorizado que labora en el área de resguardo y con ello para zonas de acceso restringido.

C.- ÁREA DE CONSULTA DE DATOS PERSONALES.

- El personal responsable de los Sistemas de Datos Personales deberá dar acceso a los datos,
- El personal responsable de los Sistemas de Datos Personales deberá verificar que el acceso solo se dé a los Titulares de los mismos sin que se tenga posibilidad de modificar o extraer los datos personales, sino solo consultarlos y bajo el procedimiento establecido en el Titulo Tercero de la LGDPPSO.
- El equipo de cómputo instalado en el área de consulta deberá cumplir con la tecnología y software para equipos de cómputo de áreas restringidas, es decir con clave o contraseñas para que únicamente acceda el usuario identificado para que realice el tratamiento que corresponda al resguardo de datos personales.

D.- PERSONAS AUTORIZADAS Y NO AUTORIZADAS.

- El personal responsable de los Sistema de Datos Personales, deberá tener un estricto control y registro de las autorizaciones emitidas para facultar al personal del CNSNS como usuario para interactuar con uno o más Sistema de Datos Personales, ya sea que, dicho personal lo haga acudiendo al área de consulta o desde otro lugar distinto, fuera de dicha área.

- El personal responsable de los Sistemas de Datos Personales, deberá registrar también la asignación, actualización y reemplazo de contraseñas de acceso y demás elementos que entregue a las y los usuarios, para que estos puedan accesar a los Sistemas Informáticos del CNSNS, lo anterior, conforme a lo que se establece n las Políticas de tecnologías de la información y comunicaciones publicadas en el D.O.F. el día 6/09/2021 donde se emiten las disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

- Cada acceso y consulta realizada por personas no autorizadas, es considerada como un incidente de intrusión, que se denunciará ante las autoridades competentes para su investigación.

MEDIDAS DE SEGURIDAD DE CARÁCTER TÉCNICO PARA DATOS PERSONALES BASADOS EN SOPORTES ELECTRÓNICOS

Las siguientes medidas de seguridad de carácter técnico su implementación es de carácter obligatorio para los Sistemas de Datos Personales de conformidad con el nivel de seguridad que les corresponda, sin limitar los controles adicionales que puedan derivarse de la elaboración de la matriz de riesgos y del análisis de brecha.

MEDIDAS DE SEGURIDAD DE CARÁCTER TÉCNICO PARA NIVEL BÁSICO.

- Los Sistemas informáticos que se usen de manera compartida por más de un usuario deberán ejecutarse en equipos de cómputo.
- Los equipo de cómputo deberán estar resguardados en el SITE de Cómputo del CNSNS.
- Para facilitar el análisis de las bitácoras, los Servidores de cómputo deberán mantener una sincronización de tiempo bajo el esquema adoptado por el CNSNS.
- Los equipos de cómputo deberán contar con un programa de mantenimiento preventivo.
- Los equipos de cómputo deberán contar con actualizaciones de seguridad periódicas.
- Los Sistemas informáticos deberán contar con evaluaciones de desempeño y seguridad.
- Los Sistemas informáticos deberán contar con Ambientes de cómputo diferentes al productivo para desarrollo y preproducción.
- Deberán utilizarse cuentas de usuario para delimitar los derechos de acceso a los Sistemas informáticos.
- Deberá llevarse a cabo de manera periódica la revisión de derechos de acceso para las cuentas de usuario.
- Los Sistemas informáticos deberán guardar bitácoras de los accesos, a sí como cambios a la información.
- Los Sistemas informáticos y bases de datos deberán contar con un Plan de respaldo. MEDIDAS DE SEGURIDAD DE CARÁCTER TÉCNICO PARA NIVEL MEDIO.

Los Sistemas informáticos que envíen información fuera del CNSNS deberán proteger la información mediante controles criptográficos.

MEDIDAS DE SEGURIDAD DE CARÁCTER TÉCNICO PARA NIVEL ALTO.

Insurgentes Sur 890, Del Valle, C.P. 03100. Benito Juárez, CDMX
t: (55) 5000.6000 www.gob.mx/sener

Los Sistemas de Datos Personales que contengan datos personales sensibles de conformidad a lo que establecen los artículos 3 fracción X, de la LGDPPSO, deberán de cumplir con las medidas de seguridad de nivel básico y medio, además de las derivadas de la matriz de riesgos y análisis de brecha para cada uno de los Datos Personales.

7.7. PROGRAMA DE CAPACITACIÓN.

Con el objeto de establecer y mantener las medidas de seguridad para la protección de los Sistemas de Datos Personales, las Unidades Administrativas del CNSNS deberán atender y cursar los diferentes niveles de capacitación, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Las acciones de capacitación tienen el propósito de que la totalidad de las personas servidoras públicas adscritas al CNSNS conozca los aspectos teóricos, conceptuales y normativos fundamentales, en materia de acceso a la información y protección de datos personales.

En ese sentido, con el objeto de atender a lo dispuesto por la LGPDPPDO y a los Lineamientos Generales, a la Política Interna de Datos Personales y al Programa de Protección de Datos Personales de la CNSNS, respecto de capacitar a las personas servidoras públicas adscritas a la CNSNS en materia de protección de Datos Personales se establecerá un Programa Anual de capacitación que deberá ser aprobado por el Comité de Transparencia del CNSNS.

VIII. INTERPRETACIÓN

La aplicación e interpretación de las presentes Políticas de Seguridad de Datos Personales de la CNSNS, son para efectos administrativos para todas las personas servidoras públicas adscritas a la CNSNS y su elaboración y el responsable de su ejecución corresponde a la UT, así como los casos no previstos.

IX. TRANSITORIOS.

PRIMERO: Las presentes Políticas de Seguridad entrarán en vigor el día siguiente de su aprobación por el Comité de Transparencia de la CNSNS.

SEGUNDO: Notifíquese las presentes Políticas de seguridad a todas las personas servidoras públicas y Unidades Administrativas adscritas a la CNSNS, difúndase al interior del Centro Nacional, publíquese en el sitio oficial de internet del Centro Nacional de Prevención de Desastres.

APROBACIÓN

El presente documento esta en revisión para su aprobación por el Comité de Transparencia de la CNSNS de conformidad con los artículos 30, 34 y 84 de la LGDPPSO.