Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES
SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES
DIRECCIÓN GENERAL DE NORMATIVIDAD Y CONSULTA

Expediente: INAI/SPDP/DGNC/EIPDP/001/2021.

Oficio: INAI/SPDP/DGNC/120/2021.

Ciudad de México, a 18 de mayo de 2021.

Asunto: Envío de dictamen de evaluación de impacto en la protección de datos personales y recomendaciones no vinculantes.

Pablo Villareal Soberanes
Titular de la Unidad de Servicios Tecnológicos y
Plataforma Digital Nacional de la Secretaría Ejecutiva
del Sistema Nacional Anticorrupción.
Domicilio: Viaducto Miguel Alemán Valdés, núm. 105, colonia Escandón Sección 1, Alcaldía Miguel Hidalgo, código postal 11800, Ciudad de México.
P r e s e n t e

Por instrucciones del Dr. Jonathan Mendoza Iserte, Secretario de Protección de Datos Personales, remito Dictamen de Evaluación de impacto en la protección de datos personales y recomendaciones no vinculantes, con relación a la puesta en operación de la Plataforma Digital Nacional, presentada mediante el oficio SE/USTPDN/009/2021 ante este Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, recaída en el expediente INAI/SPDP/DGNC/EIPDP/001/2021.

ATENTAMENTE

MDTIC. Luis Ricardo Sánchez Hernández
Director General de Normatividad y Consulta

C.c.p. Dr. Jonathan Mendoza Iserte, Secretario de Protección de Datos Personales. Para su conocimiento.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACION Y PROTECCIÓN DE DATOS PERSONALES
19 MAY 2021
1425
SECRETARÍA DE PROTECCIÓN DE DATOS PERSONALES

Recibí original.
Ricoberto Martínez Becerril
19-mayo-2021 13:30 horas.
Secretaría Ejecutiva del Sistema Nacional Anticorrupción.

En la Ciudad de México, a los dieciocho días del mes de mayo del año dos mil veintiuno; con fundamento en los artículos 74, 77 y 78 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 23, 27, 28, 29 y 30 de las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales y 42, fracciones IV y XII del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, se emite el presente:

DICTAMEN

I. Glosario.

Para efectos del presente dictamen se entenderá por:

- **Análisis para la implementación y Operación de la PDN:** Análisis para la Implementación y Operación de la Plataforma Digital Nacional[1].
- **Bases para el Funcionamiento de la PDN:** Bases para el Funcionamiento de la Plataforma Digital Nacional[2].
- **Comité Coordinador:** La instancia a la que hace referencia el artículo 113 de la Constitución Política de los Estados Unidos Mexicanos, encargada de la coordinación y eficacia del Sistema Nacional Anticorrupción.
- **Constitución:** Constitución Política de los Estados Unidos Mexicanos[3].
- **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, conforme a lo

[1] ACUERDO mediante el cual el Comité Coordinador del Sistema Nacional Anticorrupción emite el Análisis para la Implementación y Operación de la Plataforma Digital Nacional y las Bases para el Funcionamiento de la Plataforma Digital Nacional. Publicado en el Diario Oficial de la Federación el 23 de octubre de 2018, disponibles en el vínculo electrónico: https://www.dof.gob.mx/nota_detalle.php?codigo=5541802&fecha=23/10/2018, consultado por última vez el 18/05/2021.

[2] Publicadas en el Diario Oficial de la Federación el 23 de octubre de 2018, disponibles en el vínculo electrónico: https://www.dof.gob.mx/nota_detalle.php?codigo=5541802&fecha=23/10/2018, consultado por última vez el 18/05/2021.

[3] Publicada en el Diario Oficial, Órgano del Gobierno Provisional de la República Mexicana, el 05 de febrero de 1917, disponible en el vínculo: https://www.dof.gob.mx/index_113.php?year=1917&month=02&day=05, cuyo texto puede obtenerse del vínculo siguiente: http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum/CPEUM_orig_05feb1917.pdf, basado en el contenido de la información que se desprende de la imagen original disponible en el enlace: http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum/CPEUM_orig_05feb1917_ima.pdf; última reforma publicada en el Diario Oficial de la Federación el 11 de marzo de 2021, disponible en el siguiente vínculo electrónico: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_110321.pdf; texto consolidado por la Cámara de Diputados del H. Congreso de la Unión en formato de documento portable, denominado como pdf por sus siglas en inglés, incorporando las diversas reformas de dicho ordenamiento jurídico en el sitio siguiente: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_110321.pdf; enlaces consultados por última ocasión el 18/05/2021.

dispuesto en el artículo 3, fracción IX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

- **Datos personales sensibles:** Aquéllos que se refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conllevar un grave riesgo para éste. De manera enunciativa más no limitativa, se consideran sensibles aquéllos que puedan revelar aspectos como origen étnico o racial, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual de conformidad con el artículo 3, fracción X de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Derechos ARCO:** Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales, de conformidad con el artículo 3, fracción XI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Disposiciones administrativas:** Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales[4].
- **Encargado:** La persona física o jurídica, de carácter público o privado, ajena a la organización del responsable, que sola o juntamente con otras, trata datos personales a nombre y por cuenta del responsable; de conformidad con el artículo 3, fracción XV de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- **Ente público:** Los Poderes Legislativo y Judicial, los órganos constitucionales autónomos, las dependencias y entidades de la Administración Pública Federal, y sus homólogos de las entidades federativas, los municipios y alcaldías de la Ciudad de México y sus dependencias y entidades, la Procuraduría General de la República y las fiscalías o procuradurías locales, los órganos jurisdiccionales que no formen parte de los poderes judiciales, las Empresas productivas del Estado, así como cualquier otro ente sobre el que tenga control cualquiera de los poderes y órganos públicos citados de los tres órdenes de gobierno. Concepto que se incorpora únicamente como referencia en torno a dicha expresión de manera genérica.
- **Instituto o INAI:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
- **Ley General:** Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[5].

---

[4] Publicados el 23 enero de 2018, disponible para su consulta en el siguiente vínculo electrónico: https://dof.gob.mx/nota_detalle.php?codigo=5511113&fecha=23/01/2018, sin reformas; consultadas por última vez el 18/05/2021.

[5] Publicada en el Diario Oficial de la Federación, el 26 de enero de 2017, disponible en el vínculo electrónico siguiente: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017; sin reformas; texto consolidado en formato de documento portable, pdf por sus siglas en inglés, por parte de la Cámara de Diputados del H. Congreso de la Unión, en el vínculo siguiente: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf, enlaces consultados por última vez el 18/05/2021.

- **Ley General de Responsabilidades:** Ley General de Responsabilidades Administrativas[6].
- **Ley General del Sistema Nacional o del SNA:** Ley General del Sistema Nacional Anticorrupción[7].
- **Lineamientos generales:** Lineamientos Generales de Protección de Datos Personales para el Sector Público[8].
- **OIC:** Órganos Internos de Control de los Entes públicos.
- **Plataforma o PDN:** Plataforma Digital Nacional.
- **Responsable:** Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos y partidos políticos, del orden federal, que decide sobre determinado tratamiento de datos personales de conformidad con lo dispuesto en los artículos 1 y 3, fracción XXVIII de la Ley General.
- **Secretario Técnico:** El servidor público a cargo de las funciones de dirección de la Secretaría Ejecutiva, así como las demás que le confiere la presente Ley.
- **SESNA:** Secretaría Ejecutiva del Sistema Nacional Anticorrupción.
- **SNA:** Sistema Nacional Anticorrupción.
- **Titular:** Persona física a quien corresponden los datos personales conforme a lo previsto en el artículo 3, fracción XXXI de la Ley General.
- **Transferencia:** Toda comunicación de datos personales realizada a persona distinta del responsable o encargado dentro o fuera del territorio mexicano, de conformidad con el artículo 3, fracción XXXII de la Ley General.
- **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 personales, de acuerdo con lo dispuesto en el artículo 3, fracción XXXIII de la Ley General.

---

[6] Publicada en el Diario Oficial de la Federación, el 18 de julio de 2016, última reforma publicada en el Diario Oficial de la Federación el 13 de abril de 2020, disponible en los siguientes vínculos electrónicos: http://www.dof.gob.mx/nota_detalle.php?codigo=5445048&fecha=18/07/2016 y http://www.dof.gob.mx/nota_detalle.php?codigo=5591565&fecha=13/04/2020, enlaces consultado por última vez el 18/05/2021.

[7] Publicada en el Diario Oficial de la Federación, el 18 de julio de 2016, disponible en el vínculo electrónico siguiente: http://www.dof.gob.mx/nota_detalle.php?codigo=5445048&fecha=18/07/2016; sin reformas; texto consolidando en formato de documento portable, pdf por sus siglas en inglés, por parte de la Cámara de Diputados del H. Congreso de la Unión, en el vínculo siguiente: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNA.pdf, enlaces consultado por última vez el 18/05/2021.

[8] Publicados en el Diario Oficial de la Federación el 26 de enero de 2018 disponible en los siguientes vínculos electrónicos: https://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018 y http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf, última reforma publicada en el Diario Oficial de la Federación el 25 de noviembre de 2020 disponible en los siguientes vínculos electrónicos: https://www.dof.gob.mx/nota_detalle.php?codigo=5605789&fecha=25/11/2020, www.dof.gob.mx/2020/INAI/ACT-PUB-11-11-2020-05.pdf, https://home.inai.org.mx/wp-content/documentos/AcuerdosDelPleno/ACT-PUB-11-11-2020.05.pdf, enlaces consultados por última vez el 18/05/2021.

II. Antecedentes.

El 24 de marzo de 2021, la SESNA presentó ante el Instituto la evaluación de impacto en la protección de datos personales respecto a la puesta en operación de la PDN, manifestando lo siguiente:

> *"[...]*
> *Con fundamento en los artículos 74 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 10 de las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, se presenta la Evaluación de impacto en la protección de los datos personales respecto a la puesta en operación de la Plataforma Digital Nacional a que hace referencia el Título Cuarto de la Ley General del Sistema Nacional Anticorrupción.*
>
> *Para efecto de lo anterior, se relatan los siguientes:*
>
> ***ANTECEDENTES***
>
> *El artículo 74 de la Ley General de Protección de Datos Personales en posesión de sujetos obligados (**LGPDPPSO**) señala que cuando un sujeto obligado ponga en operación una plataforma informática que implique un tratamiento intensivo o relevante de datos personales deberá presentar una Evaluación de impacto de protección de datos personales ante el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos personales (**INAI**). También establece que una de las funciones del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Sistema Nacional de Transparencia), es "expedir las disposiciones administrativas necesarias para la valoración del contenido presentado por los sujetos obligados en la Evaluación de impacto en la protección de datos personales".*
>
> *En consecuencia, el Sistema Nacional de Transparencia emitió las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales. El artículo 12 de estas disposiciones administrativas especifica que cuando un sujeto obligado tenga duda respecto de la obligación de elaborar y presentar una evaluación de impacto en la protección de datos personales podrá realizar una consulta al INAI.*
>
> *Por ello, la Secretaría Ejecutiva del Sistema Nacional Anticorrupción (**SESNA**) presentó una consulta ante el INAI para determinar si existía la obligación de elaborar y presentar la Evaluación correspondiente. Como respuesta, el INAI emitió una opinión técnica en la cual concluyó que la SESNA sí está obligada a presentar la Evaluación de impacto en la protección de datos personales por la puesta en operación de **la Plataforma Digital Nacional (PDN)**. El INAI también aclaró que la evaluación debe contemplar los sistemas que se encuentren en operación. Actualmente, se encuentran en operación cuatro de los seis sistemas que conforman la PDN, por lo que la evaluación que se presenta se centra en los sistemas 1, 2, 3 y 6.*
>
> *La Plataforma se encuentra operando en su versión Beta 0.7 y, dadas sus características como una plataforma modular y escalable, se estima que **comenzará a realizar un tratamiento frecuente y continuo de grandes volúmenes de datos y cruces de información con múltiples sistemas***

> ***informáticos posterior al mes de mayo del año 2021****, fecha límite en la que todos los servidores públicos de los tres órdenes de gobierno deben presentar sus declaraciones de situación patrimonial y de intereses en los formatos aprobados para tal efecto por el Comité Coordinador del Sistema Nacional Anticorrupción, en términos de lo ordenado por el "ACUERDO por el que el Comité Coordinador del Sistema Nacional Anticorrupción da a conocer que los formatos de declaración de situación patrimonial y de intereses son técnicamente operables con el Sistema de Evolución Patrimonial y de Declaración de Intereses de la Plataforma Digital Nacional, así como el inicio de la obligación de los servidores públicos de presentar sus respectivas declaraciones de situación patrimonial y de intereses conforme a los artículos 32 y 33 de la Ley General de Responsabilidades Administrativas", publicado en el Diario Oficial de la Federación el 24 de diciembre de 2019.*
>
> *Por lo tanto, en estricta observancia a los requisitos que exige el artículo 14 de las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, se proporciona la siguiente información:*
> *[…]" (Sic)*

Como anexo a la evaluación de impacto en la protección de datos personales, la SESNA proporcionó su Documento de Seguridad.

El 07 de abril de 2021, mediante oficio número INAI/SPDP/DGNC/067/21 el Instituto solicitó a la SESNA proporcionar, por escrito, la información que a continuación se indica:

> *"[…]*
>
> ***VISTO*** *el oficio SE/USTPDN/009/2021 relacionado con la evaluación de impacto en la protección de datos personales presentada ante este Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante, INAI o Instituto) el 24 de marzo de 2021, por la Secretaría Ejecutiva del Sistema Nacional Anticorrupción (en lo sucesivo, SESNA), respecto a la puesta en operación de la Plataforma Digital Nacional (en adelante, PDN), en el cual se acompañó el Documento de Seguridad de la Secretaría Ejecutiva del Sistema Nacional Anticorrupción; así mismo, se da cuenta del ACUERDO mediante el cual se establece el calendario oficial e inhábiles del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el año 2021 y enero de 2022 publicado en el Diario Oficial de la Federación el 15 de enero de 2021, en el consideran días inhábiles y se suspenden términos en todos y cada uno de los trámites, procedimientos y de medios de impugnación competencia del Instituto, establecidos en la Ley General de Transparencia y Acceso a l Información Pública, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley Federal de Transparencia y Acceso a la Información Pública, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y demás normativa aplicable, del día lunes 29 al miércoles 31 de marzo y del jueves 1 al viernes 2 de abril; por lo cual, con fundamento en los artículos, 74, 75, y 77 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General, en adelante); 14, 24 y 25 de las Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales (en lo sucesivo Disposiciones administrativas) y 42, fracciones IV y XII del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante, Estatuto Orgánico del INAI), se emite el presente:*

ACUERDO

PRIMERO. *Se tiene por recibido el oficio SE/USTPDN/009/2021 de fecha 24 de marzo de 2021 y presentado en la misma fecha, signado por el Titular de la Unidad de Servicios Tecnológicos y Plataforma Digital Nacional de la SESNA, mediante el cual acompañó la evaluación de impacto en la protección de datos personales respecto de la Plataforma Digital Nacional, así como el anexo, consistente en copia del Documento de Seguridad de la Secretaría Ejecutiva del Sistema Nacional Anticorrupción, mismo que será devuelto al presentante una vez que se hayan concluido las actuaciones en el presente expediente .*

SEGUNDO. *Fórmese el expediente respectivo y radíquese con el número INAI/SPDP/DGNC/EIPDP/001/2021 a cargo de esta Dirección General, y glósense las constancias señaladas en el proemio del presente acuerdo.*

TERCERO. *Una vez analizados los requisitos de la Evaluación de Impacto en la Protección de Datos Personales previstos en los artículos 14, 15, 16, 17, 18, 19, 20, 21 y 22 de las Disposiciones administrativas; con fundamento en los artículos 24, fracción II y 25 del mismo ordenamiento,* ***se requiere*** *a la Secretaría Ejecutiva del Sistema Nacional Anticorrupción, para que* ***en un término de cinco días hábiles*** *contados a partir de la notificación del presente, remita por escrito a este Instituto, la información que a continuación se indica:*

1. *Con fundamento en los artículos 14, fracción I y 15, fracción III de las Disposiciones administrativas se solicita a la SESNA que describa de manera detallada los objetivos generales y específicos que persigue la puesta en operación de la Plataforma Digital Nacional, considerando todas y cada una de las funcionalidades de los sistemas que la conforman, con independencia de que dichos sistemas se encuentren en operación o no; así como la identificación de cada uno de los perfiles de usuario que utilizarán la PDN y los casos de uso y funcionalidades correspondientes, con relación a los sistemas 1, 2, 3 y 6.*
2. *Con fundamento en los artículos 14, fracción I y 15, fracción IV, de las Disposiciones administrativas, se requiere indique el fundamento legal de los siguientes sistemas y bases de datos que proveerán de información a los sistemas 1, 2, 3 y 6, objeto de análisis de la evaluación de impacto en la protección de datos personales en comento:*
    - *Sistema de Servidores Públicos de la Secretaría de la Función Pública*
    - *Registro de Servidores Púbicos del Gobierno Federal (RUSP)*
    - *Registro de Servidores Públicos de la Administración Pública Federal (RENIRESP) y de las Unidades Compradoras de CompraNet*
    - *Registro de Servidores Públicos Sancionados de la SFP (RSPS)*
    - *Plataforma de compras del Gobierno Federal, CompraNet*

Lo anterior, en virtud que, si bien, en la evaluación de impacto en la protección de datos personales se señala el fundamento legal de cuatro de los seis sistemas que conforman la PDN, por ser los que se encuentran en operación actualmente, resulta necesario identificar los elementos y requerimientos de diversos sistemas con los que tiene vinculación la Plataforma Digital Nacional, por lo que es necesario que se indique el fundamento legal de los sistemas en cita.

1. *En términos de los artículos 14, fracción I y 15, fracción V, de las Disposiciones administrativas, se solicita se señale si las categorías de titulares a los que hace referencia en cada uno de los sistemas analizados pertenecen a grupos vulnerables en función de su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica, o bien, indique expresamente la negativa de dichos supuestos para cada uno de los casos concretos.*
2. *Con fundamento en lo dispuesto por los artículos 14, fracción I y 15, fracción VI de las disposiciones administrativas, se solicita señalar expresamente a qué datos se refiere la calificación como sensibles que podrían revelar información respecto de las creencias religiosas, filosóficas u opiniones políticas sus titulares, así como los clasificados como patrimoniales en lo que respecta a la información contenida Sistema 1. Así como indicar expresamente si de los datos personales a los que se hace referencia en el resto de los sistemas, son de carácter sensible, o bien, indique expresamente la negativa de dicha característica para cada uno de los casos concretos.*
3. *En términos de los numerales 14, fracción I y 15, fracción VII de las Disposiciones administrativas, se solicita señalar lo siguiente, en cuanto a finalidades del tratamiento intensivo o relevante de datos personales refiere:*
    - *Las finalidades por las cuales, diversas autoridades competentes en la prevención, investigación y sanción de faltas administrativas y hechos da corrupción, tales como el Ministerio Público, Tribunales o autoridades judiciales, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras, entre otras, puedan solicitar y utilizar la información contenida en el Sistema 1.*
    - *Precisar si existe un cambio en la o las finalidades que justificaron el origen del tratamiento de datos personales de cada uno de los sistemas que conforman los sistemas 1, 2, 3 y 6, de tal manera que pudiera presentarse una incompatibilidad entre las finalidades de origen con las nuevas finalidades, al ser estas últimas más intrusivas para los titulares.*
    - *Detallar las finalidades en función de cada uno de los perfiles de usuarios de cada uno de los sistemas.*
4. *Con fundamento en los artículos 14, fracción I y 15, fracción VIII de las Disposiciones administrativas, se solicita señalar, de manera detallada, lo siguiente:*
    - *Las fases o etapas que conllevaría la puesta en operación de la Plataforma Digital Nacional, así como la descripción puntual de las mismas.*
    - *El proceso mediante el cual se establecerán los mecanismos de integración y conexión de la información que alimentarán los sistemas 1, 2, 3 y 6.*
    - *El proceso mediante el cual se establezcan los mecanismos para que la información de los diferentes sistemas sea consultada, solicitada y utilizada, de conformidad con los diferentes tipos de perfiles de usuarios de la PDN.*
    - *El proceso mediante el cual se realizaría la verificación aleatoria de las declaraciones patrimonial, de intereses y para identificar la evolución del patrimonio de los servidores públicos.*
    - *El proceso mediante el cual se realizaría la expedición de certificaciones de la inexistencia de anomalías que deberán anotarse en el Sistema 1.*

5. *En términos de los artículos 14, fracción I y 15, fracción IX de las Disposiciones administrativas, se solicita señalar de manera exhaustiva la forma en que se recabarán los datos personales o, en su caso, las fuentes de las cuales provienen, así como identificar y describir los actores responsables*

de los sistemas fuentes potenciales de información que proveerán y actualizarán los sistemas 1, 2, 3 y 6.

6. *Con fundamento en los numerales 14, fracción I y 15, fracción X de las Disposiciones administrativas, se requiere especificar las transferencias de datos personales que, en su caso, pretendan efectuarse con relación a la operatividad del Sistema 1, indicando lo siguiente:*
    - *Los mecanismos mediante los cuales la información del sistema sea solicitada y transferida;*
    - *Los datos personales que serán susceptibles de transferirse;*
    - *Especificar los destinatarios y las finalidades para las cuales se realizará las transferencias;*
    - *Incluir el fundamento legal que habilita las transferencias.*
7. *En términos de los artículos 14, fracción I y 15, fracción XI de las Disposiciones administrativas, se solicita señalar de manera exhaustiva el tiempo de duración de la operatividad de la Plataforma Digital Nacional, específicamente en lo correspondiente al tratamiento intensivo o relevante de datos personales. Con fundamento en los artículos 14, fracción I, y 15 fracción XII de las Disposiciones administrativas, se advierte que, a partir de la información presentada, no es posible determinar el alcance de la plataforma ya que, al ser una plataforma de interoperabilidad, no se describe a detalle la interconexión que realizará la plataforma con los sistemas enlistados. Adicionalmente, es necesario identificar al responsable o responsables de cada uno de los sistemas a fin de analizarlos y, en su caso, integrarlos al análisis de riesgos.*

   Asimismo, se informa que en los documentos presentados no se encontró el análisis a la propia plataforma dentro del documento de seguridad, por lo que se solicita información adicional, como lo pueden ser esquemas, diagramas o descripciones detalladas que permitan identificar la conectividad de la funcionalidad de la plataforma con los sistemas descritos, así como una descripción técnica que mencione la tecnología en la que se desarrolla o desarrollará la plataforma web mencionada.
8. *Con fundamento en los numerales 14, fracción I y 15, fracción XIV de las Disposiciones administrativas, se requiere señalar el nombre y cargo del servidor o de los servidores públicos que cuentan con facultad expresa para decidir, aprobar o autorizar la puesta en operación de la Plataforma Digital Nacional.*
9. *En términos de los artículos 14, fracción II y 17 de las Disposiciones administrativas, se solicita señalar expresamente las razones o motivos que justifican la necesidad de poner en operación la PDN, en función de las atribuciones que la normatividad aplicable le confiera, precisando si dicha implementación es susceptible o idónea para garantizar el derecho a la protección de datos personales de los titulares; es estrictamente necesaria, en el sentido de ser la más moderada para garantizar el derecho a la protección de datos personales de los titulares o es equilibrada en función del mayor número de beneficios o ventanas que perjuicios para el garantizar el derecho a la protección de datos personales de los titulares.*
10. *Con fundamento en los artículos 14, fracción III de las Disposiciones administrativas, se solicita señalar, manera puntual, la descripción y representación de cada una de las fases o etapas de la puesta en operación de la PDN, así como especificar el ciclo de vida de los datos personales a tratar en cada uno de los sistemas que conforma la Plataforma, a partir de su obtención, aprovechamiento, explotación, almacenamiento, conservación o cualquier otra operación realizada, hasta la supresión de los mismos. Asimismo, se deberá especificar lo siguiente:*

- *Las fuentes internas y/o externas, así como los medios, mecanismos y procedimientos a través de los cuales se recabarán los datos personales, o bien, son recabados;*
- *Las áreas, grupos o personas que llevarán a cabo operaciones específicas de tratamiento con los datos personales;*

11. *En términos de los numerales 14, fracción III y 18 fracción IV de las Disposiciones, se requiere de más información que permita identificar el funcionamiento de los sistemas que conforman la plataforma, así como de la misma plataforma a fin de identificar si es necesario describir borrado seguro de datos personales para los sistemas y el borrado de posibles datos de navegación que se generen a partir del uso de la plataforma.*
12. *Con fundamento en los artículos 14, fracción IV, y 19 de las Disposiciones Administrativas, se requiere información adicional, sobre el análisis y gestión de riesgos para la protección de datos personales de la propia plataforma, así como puntualizar la propiedad de los sistemas de conexión para complementar la información correspondiente para cada sistema.*
13. *En términos de los numerales 15, fracción XIII, y 20 de las Disposiciones Administrativas, si bien el sujeto obligado, describe las medidas de seguridad administrativas, físicas y técnicas, se advierte que a partir de la descripción de la plataforma no se identifican las medidas de seguridad de carácter físico, técnico y administrativo de la propia plataforma, y de igual manera, se requiere distinguir la propiedad de los sistemas a los que conecta la plataforma para analizarlos e incluirlos en el documento de seguridad.*
14. *Con fundamento en los artículos 14, fracción V de las Disposiciones Administrativas, se solicita se precisen los mecanismos o procedimientos que adoptarán para que la puesta en operación de la PDN cumpla, por defecto y diseño, con los principios, deberes, derechos y demás obligaciones previstas en la Ley General y demás disposiciones aplicables.*

[...]" (Sic)

El 14 de abril de 2021, mediante oficio número SE/USTPDN/0010/2021 la SESNA dio respuesta al requerimiento de información del Instituto en los siguientes términos:

"[...]

En respuesta al requerimiento de información formulado dentro del expediente INAI/SPDP/DGNC/EIPDP/001/2021, notificado mediante el oficio INAI/SPDP/DGNC/067/21, se informa lo siguiente:

[...]" (Sic)

III. Descripción de la plataforma informática PDN que se pretende poner en operación.

Conforme a lo dispuesto en el artículo 74 de la Ley General, a continuación, este Instituto realiza una descripción general de la plataforma informática PDN de acuerdo con las manifestaciones e información proporcionada por la SESNA.

La PDN es una fuente de inteligencia para construir integridad y combatir la corrupción, que creará valor para el gobierno y la sociedad a partir de grandes cantidades de datos. Es un medio que busca quitar barreras y romper silos de información para que los datos sean comparables, accesibles, oportunos e interoperables. Su construcción es modular por lo que se encuentra en constante revisión y evolución.

En este sentido, la función de la PDN es integrar y conectar diversos sistemas electrónicos que posean datos e información necesaria para que las autoridades competentes tengan acceso a los sistemas a que refiere el Título Cuarto de la Ley General del Sistema Nacional Anticorrupción. Es decir, a través de la PDN se podrá consultar en un solo espacio la información contenida en los seis sistemas legalmente establecidos.

De esta forma, la Plataforma podrá facilitar que las autoridades competentes en la prevención, detección, investigación y sanción de responsabilidades administrativas y hechos de corrupción, así como en la fiscalización y control de recursos públicos, accedan a la información necesaria para el ejercicio de sus atribuciones de manera ágil, eficiente y ordenada, así como coadyuvar a que el Comité Coordinador establezca políticas integrales y metodologías de medición e indicadores de evaluación de estas.

Al respecto, en términos del Título Cuarto de la Ley General del Sistema Nacional, la PDN estará conformada por la información que a ella incorporen los integrantes del SNA y contará con, al menos, los sistemas electrónicos siguientes:

1. Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal (en adelante, S1).
2. Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas (en lo sucesivo, S2).
3. Sistema nacional de Servidores públicos y particulares sancionados (en lo subsecuente, S3).
4. Sistema de información y comunicación del Sistema Nacional y del Sistema Nacional de Fiscalización (en adelante, S4).
5. Sistema de denuncias públicas de faltas administrativas y hechos de corrupción (en lo sucesivo, S5).
6. Sistema de Información Pública de Contrataciones (en lo subsecuente, S6).

Los seis sistemas que integrará la PDN, componen datos estratégicos necesarios para la lucha contra la corrupción, mismos que se encuentran contemplados en la Ley General del Sistema Nacional.

En este sentido, la PND se trata de una plataforma de interoperabilidad[9], que no genera ni almacena los datos, sino que a través de servicios web o Interfaces de Programación de Aplicaciones (APIs, por sus siglas en inglés)[10], consulta la información de los servidores y las bases de datos de los generadores de la información, y los refleja en la Plataforma.

En otras palabras, la PDN opera con una arquitectura basada en comunicaciones a través de Internet, que permite consultar información desde diversos proveedores de información (entes públicos), en tiempo real y de manera estandarizada (en un mismo formato).

Actualmente, se encuentra operando en su versión Beta 0.7[11] lo cual significa:

- **Beta**: Porque se encuentra en una versión preliminar, es decir, se están mejorando constantemente sus funcionalidades.
- **0.7:** Contiene datos reales de los Sistemas 1, 2, 3, y 6 y se logró la interconexión con algunos de los sujetos obligados.

Actualmente, se encuentran en operación cuatro de los seis sistemas que conforman la PDN, por lo que, el análisis del presente Dictamen de la evaluación que se presentó por el SESNA se centra de manera particular en los sistemas 1, 2, 3 y 6, con independencia de que se emitan consideraciones generales con relación a los sistemas 4 y 5, atendiendo a las interacciones que entre estos se realicen.

En este sentido y tomando en consideración lo señalado por la SESNA en el análisis para la implementación y operación de la Plataforma Digital Nacional, cabe señalar que:

- **La PDN no es un repositorio de datos**. La Plataforma no es un mecanismo de recopilación de datos, ni tampoco de resguardo de estos. En contraposición, es un portal de consulta de información interoperable para los usuarios que establece la normativa que le da origen, es decir, a través de la Plataforma se podrá consultar en un solo espacio la información contenida en los seis sistemas legalmente establecidos.
- **La PDN no es una herramienta primordialmente de consulta pública**. Como se ha mencionado, la PDN es una herramienta del SNA que busca consolidarse como fuente primigenia y fidedigna de consulta de la información y los datos que requieran los usuarios

[9] De conformidad con el artículo 3, fracción XV de las Bases para el funcionamiento de la PDN, se entiende como interoperabilidad a: La capacidad de organizaciones, sistemas y datos, dispares y diversos, para interactuar con objetivos consensuados, a través de estándares comunes, con la finalidad de obtener beneficios mutuos, en donde la interacción implica que las dependencias y entidades compartan infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas de tecnología de información y comunicaciones.

[10] Entendiéndose como API, un conjunto de definiciones y protocolos que se utiliza para desarrollar e integrar el software de las aplicaciones. Las API permiten que sus productos y servicios se comuniquen con otros, sin necesidad de saber cómo están implementados. Esto simplifica el desarrollo de las aplicaciones y permite ahorrar tiempo y dinero.

[11] De acuerdo con la aclaración expuesta en el sitio web de la Plataforma Digital, disponible en el siguiente vínculo electrónico: https://plataformadigitalnacional.org/terminos consultado por ultima vez el 18/05/2021.

focalizados. En este sentido, a pesar de que se insta en que la información que contiene la Plataforma sea, en la medida de lo posible, de carácter público y reportada en formato de datos abiertos, **su principal función debe entenderse como herramienta de generación de inteligencia institucional y no como portal de acceso a información pública**.

Ahora bien, de los seis sistemas que conforman la PDN, es preciso señalar lo siguiente:

Sistema 1. Sistema de evolución patrimonial de declaración de intereses y constancia de presentación de declaración fiscal.

Será en el S1 donde se tendrá acceso a los datos de servidores públicos obligados a presentar las declaraciones patrimoniales y de intereses, a la que se incluirá también la constancia que emita la autoridad fiscal sobre la declaración de impuestos. Es decir, en el S1 de la Plataforma se integrarán las tres declaraciones. Estos datos serán estandarizados de acuerdo con las especificaciones emitidas por la SESNA.

En este sentido, la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos, según corresponda, se deben coordinar con la SESNA para establecer los mecanismos de integración y conexión de la información contenida en los sistemas electrónicos a través de los cuales los servidores públicos presenten las declaraciones. Lo anterior se contempla en el artículo 41 de las enunciadas Bases de la PDN.

Es importante especificar que son dos tramos diferentes relacionados con la presentación y registro de las declaraciones patrimoniales, que utilizan dos herramientas diferentes. Por un lado, las herramientas a través de las cuales la Secretaría de la Función Pública y sus homólogos en las entidades federativas, así como OICs de los Entes públicos reciben la información por parte de las y los servidores públicos, y por otro, el propio S1, que estará a cargo de la SESNA.

Por tanto, el S1 de la Plataforma no reemplazará a los sistemas de recepción de las declaraciones patrimoniales y de intereses que corresponden a las Secretaría de la Función Pública y sus homólogos en las entidades federativas y a los OICs mantener registrados y actualizados, respecto de las/los declarantes a su cargo.

Por lo anterior, se puede afirmar que la PDN no es el medio a través del cual se implementan las declaraciones, sino que serán los sujetos obligados los que determinarán qué plataforma, sistema o mecanismo utilizan para realizar sus declaraciones, no obstante, la SESNA estará encargada de

establecer los mecanismos de integración y conexión a la PDN de la información contenida en dichos sistemas electrónicos.

Asimismo, respecto a la información contenida en este sistema es preciso advertir que se debe dividir la información en pública y reservada, de acuerdo con lo aprobado por el Comité Coordinador. En esta etapa de la PDN solo se cuenta con información de carácter público. Hasta que no se apruebe y publique el catálogo de perfiles -que establecerá quiénes son los usuarios que podrán acceder a la información reservada, conforme a la normativa aplicable- la PDN no permitirá la consulta y el intercambio de los datos reservados.

Adicionalmente, la SESNA será la encargada de establecer **los mecanismos para que la información del sistema sea solicitada y utilizada** de acuerdo con las necesidades de las diversas autoridades competentes, como el Ministerio Público, Tribunales o autoridades judiciales, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras, entre otras, en el ejercicio de sus respectivas atribuciones, previa aprobación del Comité Coordinador.

De igual forma, la SESNA establecerá un portal del sistema para dar acceso a la **información pública** de las declaraciones de situación patrimonial y de intereses a todos los ciudadanos.

Finalidades del S1:

- Que la información del sistema pueda ser solicitada y utilizada de acuerdo con las necesidades de las diversas autoridades competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción, entre las que se encuentran el Ministerio Público, Tribunales o autoridades judiciales, servidores públicos, autoridades investigadoras, sustanciadores o resolutoras, entre otras.
- Dar acceso a la **información pública** de las declaraciones de situación patrimonial y de intereses a todos los ciudadanos.
- Permitir que la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los OICs de los Entes públicos realicen la verificación aleatoria de las declaraciones patrimonial, de intereses, y para identificar la evolución del patrimonio de los servidores públicos.
- Permitir la expedición de certificaciones de la inexistencia de anomalías de las declaraciones presentadas por los servidores públicos, las cuales deberán anotarse en el sistema.

Titulares de los datos personales en S1:

a) Declarante, servidores públicos en términos del artículo 108 de la Constitución Política de los Estados Unidos Mexicanos, no pertenecen a un grupo vulnerable.
b) Terceros con relación directa del Servidor Público declarante:
    i. Cónyuge
    ii. Dependientes económicos.
c) Clientes principales del Servidor Público declarante, con la información que se incluirá en el sistema no podrían ser calificados como grupo vulnerable.
d) Terceros relacionados con el declarante, tales como:
    i. Tercero cuando se trate de copropiedad sobre vehículos, bienes inmuebles, bienes muebles, inversiones, cuentas bancarias y otro tipo de valores/activos.
    ii. Tercero cuando se trate de una co- deuda.
    iii. Transmisor de la propiedad de vehículos, bienes inmuebles, bienes muebles.
    iv. Otorgante de beneficios privados.
    v. Representante/representado.
    vi. Fideicom tente.
    vii. Fiduciario.
    viii. Fideicomisario.

Datos personales en el S1:

En este sentido, los datos personales que serán objeto de tratamiento respecto del S1 se encuentran relacionados con los datos que se solicitan en los formatos de declaraciones de situación patrimonial y de intereses solicitados al titular servidor público declarante y son:

1) Datos del declarante:

- Nombre.
- Primer y segundo apellido.
- Clave Única de Registro de Población (CURP).
- Registro Federal de Contribuyentes (RFC) y homoclave.
- Correo electrónico institucional.
- Correo electrónico personal/alterno.
- Número telefónico de casa.
- Número celular personal.
- Régimen matrimonial.
- Estado Civil.
- País de nacimiento.
- Fecha de nacimiento.
- Nacionalidad.

- Firma.
- Domicilio.
- Escolaridad (último grado de estudios).
- Institución educativa donde se realizaron los estudios.
- Lugar donde se ubica la institución educativa.
- Carrera o área de conocimiento.
- Estatus.
- Fecha de obtención del documento.
- Documento obtenido.
- Empleo/cargo/comisión.
- Nivel del empleo, cargo o comisión.
- Función o actividad principal que desempeña en su empleo, cargo o comisión.
- Fecha de toma de posesión/conclusión del empleo, cargo o comisión.
- Nombre del ente público al cual se encuentra adscrita la plaza.
- Área de adscripción.
- Ámbito público.
- Nivel/orden de gobierno.
- Teléfono de oficina y extensión.
- Domicilio del empleo, cargo o comisión.
- Experiencia laboral.
- Años laborados.
- Ámbito/sector en el que se laboró.
- Ingresos netos del declarante.
- Bienes inmuebles.
- Vehículos.
- Bienes muebles.
- Inversiones.
- Cuentas bancarias.
- Otro tipo de valores/activos.
- Adeudos/pasivos.
- Préstamo o comodato por terceros.
- Participación en empresas, sociedades, asociaciones.
- Apoyos o beneficios públicos.
- Beneficios privados.
- Fideicomisos.
- Representación.

2) **Datos del cónyuge del declarante:**

- Nombre.
- Primer y segundo apellidos.
- CURP.
- RFC y homoclave.
- Relación con el declarante.
- Estado civil.
- Lugar de nacimiento.
- Fecha de nacimiento.
- Nacionalidad.
- Lugar de residencia.
- Domicilio.
- Actividad laboral.
- Lugar de trabajo.
- Ingresos netos.
- Otros ingresos.
- Bienes inmuebles.
- Vehículos.
- Bienes muebles.
- Inversiones, cuentas bancarias u otro tipo de valores /activos.
- Adeudos/pasivos.
- Préstamo o comodato por terceros.
- Participación en empresas, sociedades, asociaciones.
- Apoyos o beneficios públicos.
- Beneficiarios privados.
- Fideicomisos.
- Representación.

3) **Datos de los dependientes económicos del declarante:**

- Nombre completo.
- Primer y segundo apellidos.
- CURP.
- RFC y homoclave.
- Parentesco con el declarante.
- Lugar de nacimiento.

- Fecha de nacimiento.
- Nacionalidad.
- Lugar de residencia.
- Domicilio.
- Actividad laboral.
- Lugar de trabajo.
- Ingresos netos.
- Otros ingresos.
- Bienes inmuebles.
- Vehículos.
- Bienes muebles.
- Inversiones, cuentas bancarias u otro tipo de valores /activos.
- Adeudos/pasivos.
- Préstamo o comodato por terceros.
- Participación en empresas, sociedades, asociaciones.
- Apoyos o beneficios públicos.
- Beneficiarios privados.
- Fideicomisos.
- Representación.

4) Datos de los clientes principales del servidor público/pareja/dependiente económico:

- Nombre completo.
- RFC.
- Sector productivo al que pertenece.
- Servicio que proporciona.
- Lugar donde se ubica.

5) Datos de terceros relacionados con el declarante:

- Nombre completo.
- RFC.
- Dato que permita su identificación.
- Relación del transmisor del vehículo con el titular.
- Relación del transmisor de la propiedad con el titular.
- Relación con el dueño o titular.

Asimismo, respecto a la información contenida en el S1 es preciso advertir que se debe dividir la información en pública y reservada, de acuerdo con lo aprobado por el Comité Coordinador. En esta etapa de la PDN solo se cuenta con información de carácter público. Hasta que no se apruebe y publique el catálogo de perfiles -que establecerá quiénes son los usuarios que podrán acceder a la información reservada, conforme a la normativa aplicable- la PDN no permitirá la consulta y el intercambio de los datos reservados.

Asimismo, conviene traer a colación que la información contenida en el S1 es susceptible de ser transferida a las diversas autoridades de los tres órdenes de gobierno, competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción, entre las que se encuentran el Ministerio Público, órganos jurisdiccionales como el Tribunal Federal de Justicia Administrativa y sus homólogos en las entidades federativas, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras a las que alude la Ley General de Responsabilidad, como la Secretaria de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los OICs de los Entes públicos.

S2: Sistema de los servidores públicos que intervengan en procedimientos de contrataciones públicas.

La Ley General de Responsabilidades, en su artículo 43, establece la creación del S2, que deberá utilizar los formatos y mecanismos determinados por el Comité Coordinador para registrar la información sobre los nombres y la adscripción de servidoras y servidores públicos que participen en procedimientos de contratación pública y que realicen la tramitación, atención y/o resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos.

Dicha información estará puesta a disposición de todo el público a través de un portal de internet.

El S2 estará conformado por la siguiente información:

- Nombres y adscripción de los servidores públicos que intervengan en contrataciones de acuerdo con los formatos especificados por el Comité Coordinador.
- Incluirá la relación de particulares, personas físicas y morales, que se encuentren inhabilitados para celebrar contratos con entes públicos, derivado de procesos administrativos, de acuerdo con el artículo 44 de la Ley General de Responsabilidades.

Finalidades del S2:

- Los distintos usuarios tengan acceso a la información relacionada con los servidores públicos que intervienen en procedimientos de contrataciones públicas, de tal manera que sea utilizada por los integrantes del SNA y autoridades competentes en sus funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos para ejercer sus facultades.
- Permitir que el público en general usuarios tenga acceso a la información relacionada con los servidores públicos que intervienen en procedimientos de contrataciones públicas.

Titulares de los datos personales en el S2:

a) Servidores Públicos en términos del artículo 108 de la Constitución Política de los Estados Unidos Mexicanos que intervengan en contrataciones públicas.
b) Particulares, personas físicas y morales, que se encuentren inhabilitados para celebrar contratos con entes públicos, derivado de procesos administrativos, de acuerdo con el artículo 44 de la Ley General de Responsabilidades.

Datos personales en el S2:

Ahora bien y conforme a lo antes expuesto, el Instituto advierte que los datos personales que serán objeto de tratamiento respecto del S2 refieren a servidores públicos relacionados con procedimientos de contrataciones públicas y particulares, personas físicas y morales, que se encuentren inhabilitados para celebrar contratos con entes públicos, son los siguientes:

Datos de servidores públicos que intervienen en procedimientos de contrataciones públicas:

- Nombre completo del servidor público.
- Nombre completo de la persona servidora pública que funge como superior jerárquico.
- RFC del servidor público.
- CURP del servidor público.
- RFC de la persona servidora pública que funge como superior jerárquico.
- CURP persona servidora pública que funge como superior jerárquico.

Datos de particulares, personas físicas y morales, que se encuentren inhabilitados para celebrar contratos con entes públicos:

- Nombre.
- RFC.

- Tipo de falta.
- Causas, motivos o hechos de sanción.

Adicionalmente, cabe mencionar que la SESNA manifestó que no se realizarán transferencias de datos personales por lo que refiere al tratamiento de datos personales llevados a cabo a través del S2.

S3: Sistema Nacional de servidores públicos y particulares sancionados.

En el S3 se inscribirán y se harán públicas, las constancias de sanciones o de inhabilitación que se encuentren firmes en contra de los servidores públicos o particulares que hayan sido sancionados por actos vinculados con faltas graves en términos de la Ley General de Responsabilidades, así como la anotación de aquellas abstenciones que hayan realizado las autoridades investigadoras o las salas especializadas en materia de Responsabilidades Administrativas de los tribunales de justicia administrativa del país.

En este sentido, en el tercer sistema de la PDN, estará conformado por:

- El registro de las constancias de sanciones impuestas tanto a servidoras y servidores públicos, como a particulares por la comisión de faltas administrativas o hechos de corrupción, en términos de la Ley General de Responsabilidades y de la legislación penal.
- La relación de los particulares, personas físicas y morales, que se encuentren inhabilitados para celebrar contratos con los entes públicos derivado de procedimientos administrativos diversos a los previstos por la Ley de Responsabilidades.
- La anotación de aquellas abstenciones que hayan realizado las autoridades investigadoras o el Tribunal Federal de Justicia Administrativa en términos de los artículos 77 y 80 de la Ley de Responsabilidades.

Finalidades del S3:

- Permitir que los usuarios tengan acceso a los datos relacionados con sanciones impuestas a servidores públicos y particulares por la comisión de faltas administrativas graves, en términos de la Ley General de Responsabilidades Administrativas, y hechos de corrupción, en términos de la legislación penal aplicable, a fin de hacer disponible dicha información para que sea utilizada por los integrantes del SNA y autoridades competentes en la prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.

- Que los Entes públicos, previo al nombramiento, designación o contratación de quienes pretendan ingresar al servicio público, consulten el S3, con el fin de verificar si existen inhabilitaciones de dichas personas.
- Permitir que el público en general tenga acceso a la información relacionada con los servidores públicos que intervienen en procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos.

Titulares de los datos personales en el S3:

a) Servidores públicos en términos del artículo 108 de la Constitución Política de los Estados Unidos Mexicanos, sancionados.
b) Particulares sancionados.

Datos personales en el S3:

Ahora bien y conforme a lo antes expuesto, el Instituto advierte que los datos personales que serán objeto de tratamiento respecto del S3 refieren a servidores públicos y particulares sancionados, son los siguientes:

Datos personales de servidor público sancionado:

- Nombre del servidor público sancionado.
- Género servidor público sancionado.
- RFC servidor público sancionado.
- CURP servidor público sancionado.
- Dependencia.
- Tipo de falta.
- Causas, motivos o hechos de la sanción.
- Tipo de sanción.

Datos personales de particulares sancionados:

- Nombre del particular sancionado.
- RFC del particular sancionado.
- Dependencia.

- Tipo de falta.
- Causas, motivos o hechos de la sanción.
- Tipo de sanción.

Adicionalmente, cabe mencionar que la SESNA manifestó que no se realizarán transferencias de datos personales por lo que refiere al tratamiento de datos personales llevados a cabo a través del S3.

S6: Sistema de Información Pública de Contrataciones.

Este sistema comprenderá la información que remitan las autoridades al Comité Coordinador y deberá contener al menos, información relacionada con la planeación, los procedimientos de contratación y los datos relevantes y la ejecución de los contratos de adquisiciones, arrendamientos, servicios, obras públicas y servicios relacionados con las mismas.

Al respecto, el S6 de la PDN, estará conformado por:

- Información relacionada con la planeación, los procedimientos de contratación y los datos relevantes y la ejecución de los contratos de adquisiciones, arrendamientos, servicios, obras públicas y servicios relacionados con las mismas otorgada por los encargados.
- Los datos derivados del manifiesto de vínculos o relaciones de negocios, personales o familiares, así como de posibles conflictos de interés que tengan los particulares, de acuerdo con lo establecido en el protocolo de actuación en contrataciones que al efecto emita el Comité Coordinador de acuerdo con la Ley General de Responsabilidades.

Finalidades del S6:

- Permitir que los distintos usuarios tengan acceso a la información pública de contrataciones, de tal manera que sea utilizada por los entes públicos y los integrantes del SNA en las funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.
- Que pueda ser consultada por la ciudadanía en general.

Titulares de los datos personales en el S6:

a) Servidores públicos que intervienen en los procedimientos de contrataciones públicas.
b) Personas físicas o morales que participan en procedimientos de contrataciones públicas.
c) Personas físicas o morales a las que se les adjudica un contrato público.

Datos personales en el S6:

Ahora bien y conforme a lo antes expuesto, el Instituto advierte que los datos personales que serán objeto de tratamiento respecto del S6 refieren a servidores públicos y particulares que intervienen y participan en los procedimientos de contrataciones públicas, y personas físicas a las que se les adjudica un contrato público son los siguientes:

- Nombre de las personas servidoras públicas que intervienen en los procedimientos de contrataciones públicas.
- Nombre de las personas físicas que participan en procedimientos de contrataciones públicas.
- Nombre de las personas físicas a las que se las adjudica un contrato público.

Adicionalmente, cabe mencionar que la SESNA manifestó que no se realizarán transferencias de datos personales por lo que refiere al tratamiento de datos personales llevados a cabo a través del S6.

Actores involucrados en la operación y funcionamiento del PDN:

Ahora bien, es importante mencionar que, como parte del análisis realizado de los elementos presentados por la SESNA, se pueden identificar diferentes actores involucrados en su operación y funcionamiento, a saber:

- **Encargado (a nivel federal, estatal y municipal):** tendrán la obligación de actualizar y administrar los subsistemas y de cumplir la normativa que señale la SESNA para garantizar la estandarización, integridad e interoperabilidad de la información de los sistemas de la Plataforma.
- **Concentradores (a nivel federal, estatal y municipal):** tendrán la obligación de agrupar la información proporcionada por los proveedores en los conjuntos de datos para que sea ingresada a los sistemas o subsistemas, según corresponda.
  Será obligación de los encargados y los concentradores vigilar la homologación, actualización y disponibilidad de la información que sea transferida de los subsistemas y conjuntos de datos a los sistemas, de conformidad con la normatividad aplicable, y verificar de manera permanente el correcto funcionamiento de los subsistemas y conjuntos de datos, así como sus procesos de generación, estandarización, actualización y distribución de información a los sistemas, de acuerdo con las disposiciones emitidas por la SESNA, para asegurar el correcto funcionamiento de la Plataforma.
- **Proveedores (a nivel federal, estatal y municipal) de la información** que estará integrada en la PDN especificando que la información que deberá contener la PDN es la que a ella

incorporen los integrantes del SNA. Es así que los proveedores de la plataforma son los sistemas de recopilación y generación de datos de la APF, el órgano garante del acceso a la información a nivel nacional (INAI), la Auditoría Superior de la Federación, el Poder Judicial Federal, así como las entidades estatales y municipales que conformen los SLA.

- **Usuarios:** autoridades con atribuciones y facultades para hacer uso de los sistemas de la PDN y/o para ejercer derechos o acceder a la información, conforme a la normativa aplicable, así como público en general.

Aunado a lo anterior, y de conformidad con lo manifestado por la SESNA, es posible advertir la identificación de los siguientes usuarios de la PDN:

S1.

- Ministerios públicos.
- Tribunales o autoridades judiciales.
- Autoridades investigadoras, substanciadores o resolutoras que requieran información con motivo de investigaciones o la resolución de procedimientos de responsabilidades administrativas.
- Secretaría de la Función Pública y sus homólogos en las entidades federativas.
- OICs de los entes públicos.
- Servidores públicos declarantes.
- Público en general.

S2.

- Integrantes del SNA y autoridades competentes en sus funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.
- Público en general.

S3.

- Integrantes del SNA y autoridades competentes en sus funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.
- Servidores públicos de los Entes públicos.
- Público en general.

S6.

- Integrantes del SNA y autoridades competentes en sus funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.
- Servidores públicos de los entes públicos.
- Público en general.

No obstante, la SESNA informó que actualmente no se cuenta con un catálogo de perfiles de usuarios, ya que el mismos se encuentra en proceso de elaboración. En ese sentido, a través del presente se establece de manera enunciativa quiénes son los perfiles de usuarios de la PDN y las funcionalidades de acuerdo con cada perfil; asimismo, se definirán los perfiles que podrán acceder a la información reservada del S1, conforme a la normativa aplicable. Por lo que, en esta etapa de la plataforma, únicamente se podrá acceder al componente público y no se permitirá la consulta y el intercambio de los datos reservados.

Por lo que refiere a los proveedores de la información (entes públicos), es importante mencionar que la SESNA no proporcionó más información relacionada con los proveedores de la información. No obstante, a efecto de contar con mayores elementos a efectos de emitir el presente dictamen, este Instituto pudo advertir, del análisis del documento denominado Análisis para la implementación y operación de la PDN, lo siguiente:

Proveedores del S1.

- Las y los servidores públicos declarantes quienes tienen la obligación de presentar las declaraciones de situación patrimonial y de intereses en el portal de este sistema.
- Las Secretarías y los órganos internos de control, que son los responsables de recibir y concentrar las declaraciones presentadas por las y los servidores públicos.
- El Servicio de Administración Tributaria, quien tendrá la obligación de brindar dos tipos de información: la relativa a la firma electrónica y la constancia de presentación de la declaración fiscal que presente la o el servidor público. Asimismo, la firma electrónica emitida por el SAT sirve para firmar tanto la declaración fiscal en el portal del SAT, como las declaraciones de situación patrimonial y la de intereses.

Proveedores del S2.

- Las áreas de recursos humanos de los entes públicos que cuentan con un registro actualizado de sus servidores públicos, incluyendo bases de datos con información que refiere a sus servidores públicos involucrados en contrataciones públicas.
- Las dependencias que cuentan con la atribución de concentrar la información en materia de recursos humanos de cada uno de los poderes y organismos autónomos.

A nivel federal, cada dependencia cuenta con un área de recursos humanos, la cual actualiza periódicamente su base de datos de servidores públicos involucrados en contrataciones públicas. Periódicamente, las áreas de recursos humanos envían las actualizaciones de sus bases de datos de recursos humanos a la Unidad de Política de Recursos Humanos de la APF, de la Secretaría de la Función Pública, la cual tiene facultad de incorporarlos al Registro de Servidores Públicos de la Administración Pública Federal.

Proveedores S3.

- La Secretaría de a Función Pública, las contralorías estatales, así como los OIC de todos los entes públicos y sus equivalentes en las entidades federativas.
- El Tribunal Federal de Justicia Administrativa a través de las sanciones impuestas a particulares y a servidores públicos por faltas administrativas marcadas como graves en la Ley General de Responsabilidades.
- Respecto de los hechos de corrupción, corresponderia al Consejo de la Judicatura registrar las penas impuestas; no obstante, también la Fiscalia Especializada en Combate a la Corrupción, al contar con la información respectiva podría ser el ente proveedor del sistema.

Proveedores S6.

- Las y los servidores públicos que operan los sistemas transaccionales de contrataciones.
- Las y los servidores públicos que participan y generan información en los procedimientos de contrataciones.
- Las personas fís cas y morales, potencialmente licitantes, proveedores y contratistas.

Por otro lado, la SESNA señaló que cada sistema de la PDN que actualmente opera se alimentará de distintas bases de datos, los cuales serán parte fundamental de la información a la que tendrá acceso el SNA a través de la Plataforma.

- **S1** se alimentará, principalmente, del Sistema de Evolución Patrimonial de Declaración de Intereses y Constancia de Prestación de Declaración Fiscal mejor conocido como DeclaraNet.
- **S2** se alimentará del Registro de Servidores Púbicos del Gobierno Federal, el Registro de Servidores Públicos de la Administración Pública Federal que intervienen en procedimientos de contrataciones públicas y de las Unidades Compradoras de CompraNet.
- **S3** se alimentará del Registro de Servidores Públicos Sancionados; Sistema de procedimientos administrativos de responsabilidades y el Sistema Integral de Responsabilidades Administrativas.
- **S6** se alimentará de CompraNet y la Bitácora Electrónica de Obra Pública.

Finalmente, es posible advertir tres posibles fases en el tratamiento de datos personales: la primera, la integración y conexión de los diversos sistemas; la segunda, la consulta a dicha información por parte de los diferentes perfiles de usuarios, y finalmente la tercera fase que corresponde a la consulta, disposición e intercambio de información que determinados usuarios tendrán de la misma. En esta fase, se encuentra incluida los datos personales de carácter confidencial del S1.

IV. Marco normativo aplicable a las evaluaciones de impacto en la protección de datos personales.

IV.1. Fundamento.

Los artículos 3, fracción XVI, 74, 75, 76, 77 y 78 de la Ley General, los artículos 1, 6, 7, 8, 9, 10, 14, 23, 27, 28, 29 y 30 de las Disposiciones administrativas, las cuales disponen que la Ley General tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos y fideicomisos y fondos públicos en los tres órdenes de gobierno, destacando que dicho ordenamiento resulta directamente aplicable en el ámbito federal.

Específicamente, una evaluación de impacto en la protección de datos personales es un documento mediante el cual cualquier responsable que pretenda poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, valora los impactos reales de dicho tratamiento de datos personales a efecto de identificar y mitigar posibles riesgos relacionados con el cumplimiento de los principios, deberes y derechos previstos en la normativa aplicable.

Ahora bien, el responsable estará en presencia de un tratamiento intensivo o relevante de datos personales cuando concurran las siguientes condiciones:

- Existan riesgos inherentes a los datos personales a tratar.
- Se traten datos personales sensibles a los que se refiere el artículo 3, fracción X de la Ley General.
- Se efectúen o pretendan efectuar transferencias de datos personales a las que se refiere el artículo 3, fracción XXXII de la Ley General.

Asimismo, el responsable estará en presencia de tratamientos intensivos o relevantes de datos personales específicos cuando pretenda realizar alguna de las siguientes acciones:

- Cambiar la o las finalidades que justificaron el origen de determinado tratamiento de datos personales, de tal manera que pudiera presentarse una incompatibilidad entre las finalidades de origen con las nuevas finalidades, al ser estas últimas más intrusivas para los titulares.
- Evaluar, monitorear, predecir, describir, clasificar o categorizar la conducta o aspectos análogos de los titulares, a través de la elaboración de perfiles determinados para cualquier finalidad, destinados a producir efectos jurídicos que los vinculen o afecten de manera significativa, especialmente, cuando a partir de dicho tratamiento se establezcan o pudieran establecerse diferencias de trato o un trato discriminatorio económico, social, político, racial, sexual o de cualquier otro tipo que pudiera afectar la dignidad o integridad personal de los titulares.
- Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa más no limitativa, a su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica.
- Crear bases de datos respecto de un número elevado de titulares de tal manera que se produzca una acumulación no intencional de una gran cantidad de datos personales respecto de los mismos.
- Incluir o agregar nuevas categorías de datos personales a las bases de datos ya existentes y en posesión del responsable, de tal forma que, en caso de presentarse una vulneración a la seguridad pudiera derivarse una afectación a la esfera personal de los titulares.
- Realizar un tratamiento frecuente y continúo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.
- Utilizar tecnologías con sistemas de vigilancia; aeronaves o aparatos no tripulados; mineria de datos; biometría; Internet de las cosas; geolocalización; técnicas analíticas; radiofrecuencia o cualquier otra que pueda desarrollarse en el futuro y que implique un tratamiento de datos personales a gran escala.
- Realizar transferencias internacionales de datos personales a países que no cuenten en su derecho interno con garantías suficientes y equivalentes para asegurar la debida protección de los datos personales, conforme al sistema jurídico mexicano en la materia.
- Revertir la disociación de datos personales para la consecución de finalidades determinadas, especialmente si éstas son de carácter intrusivo o invasivo al titular, entre otros.

Es por ello, que cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que, a su juicio y de conformidad con la Ley General y las Disposiciones administrativas, impliquen un tratamiento intensivo o relevante de datos personales está obligado a presentar una evaluación de impacto en la protección de datos personales ante el Instituto, al menos, con treinta días hábiles de

anterioridad a la fecha en que se pretenda poner en operación o modificar la política pública, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología.

Una vez presentada la evaluación de impacto en la protección de datos personales conforme a lo anteriormente descrito, el Instituto está obligado a valorar la misma tomando en consideración lo siguiente:

- Los objetivos generales y específicos que persigue la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.
- Las razones o motivos que justifican la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, en función de las atribuciones o facultades del responsable que la normatividad aplicable le confiera.
- Las categorías de titulares, distinguiendo aquéllos que pertenezcan a grupos vulnerables en función de su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica.
- Los datos personales tratados y su volumen.
- Las finalidades del tratamiento intensivo o relevante de datos personales.
- Las transferencias, nacionales o internacionales, de datos personales que, en su caso, pretendan efectuarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.
- La tecnología utilizada para efectuar el tratamiento intensivo o relevante de datos personales.
- Las medidas de seguridad de carácter administrativo, físico y técnico que se pretenden adoptar.
- Los posibles riesgos y amenazas, así como el daño o consecuencias que pudieran producirse o presentarse si llegasen a materializarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.
- Las medidas y controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos identificados.
- Los mecanismos o procedimientos que adoptará el responsable para que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumpla, desde el diseño y por defecto, con las obligaciones previstas en la Ley General y demás disposiciones aplicables.

- La opinión técnica del oficial de protección de datos personales respecto del tratamiento intensivo o relevante de datos personales que implique la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, en su caso.
- Cualquier otra información que considere pertinente atendiendo a las circunstancias del caso en particular.

Para tal efecto, el Instituto está obligado a emitir un dictamen, dentro de los treinta días hábiles posteriores al día siguiente de la presentación de la evaluación de impacto en la protección de datos personales, determinando que:

- La política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales cumple con lo dispuesto en la Ley General y demás disposiciones aplicables, y, por lo tanto, no será necesario emitir recomendaciones no vinculantes al respecto, o
- La política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales no cumple con lo dispuesto en la Ley General y demás normatividad aplicable, y, por lo tanto, será necesario emitir recomendaciones no vinculantes al respecto.

Cabe señalar, que el dictamen emitido por el Instituto no tendrá el efecto de impedir la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales en cuestión, como tampoco validar el presunto cumplimiento de las obligaciones previstas en la Ley General y demás disposiciones aplicables en perjuicio de las atribuciones conferidas al Instituto. Lo anterior, en virtud de que el objeto de este tipo de evaluaciones es orientar a los responsables sobre el fortalecimiento y mejor cumplimiento de las obligaciones en la materia mediante la emisión de recomendaciones no vinculantes.

Aunado a lo anterior, el análisis y recomendaciones realizadas por el Instituto en el presente dictamen se efectúan a partir de la información presentada por la SESNA, por lo que esta unidad administrativa se limita a realizar recomendaciones y observaciones sobre los mecanismos o procedimientos para que la puesta en operación de la PDN cumpla con las obligaciones previstas en la Ley General y demás disposiciones aplicables en la materia.

Asimismo, este análisis no incluye pruebas de penetración ni peritajes a la PDN por lo que las manifestaciones del Instituto no pueden entenderse como vistos buenos a la implementación de medidas de seguridad, sino que se limitan a realizar recomendaciones y observaciones sobre la seguridad de los datos personales a nivel documental; supuestos de análisis que se encuentran

reconocidos de manera expresa en la Ley General y en las Disposiciones administrativas, bajo la lógica no sólo del trámite establecido expresamente para este procedimiento, sino del resultado de la Dictaminación, hacia la eventual emisión de recomendaciones no vinculantes.

IV.2. Objeto, alcance y salvedades.

Establecido el marco de contexto de la procedencia y tramitación de las Evaluaciones de impacto en la protección de datos personales, es posible advertir que, en términos de lo dispuesto por los artículos 3, fracción XVI, 74, 75 y 76 de la Ley General, 120 de los Lineamientos generales, y, 8 y 9 de las Disposiciones administrativas, la obligación de elaboración y presentación de dicho documento se genera a partir de los siguientes supuestos:

- Puesta en operación o modificación.
- Políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología.
- Implique el tratamiento intensivo o relevante de datos personales; de carácter general, particular, o ambos.

Por su parte, en términos de los artículos 48 y 49 de la Ley General del SNA el Comité Coordinador emitirá las bases para el funcionamiento de la PDN que permita cumplir con los procedimientos, obligaciones y disposiciones señaladas en la Ley General del SNA y la Ley General de Responsabilidades Administrativas, así como para los sujetos de la Ley General del SNA, atendiendo a las necesidades de accesibilidad de los usuarios. La Plataforma Digital Nacional será administrada por la Secretaría Ejecutiva, a través del Secretario Técnico en los términos de la Ley General del SNA.

La PDN estará conformada por la información que a ella incorporen las autoridades integrantes del Sistema Nacional y contará, al menos, con los siguientes sistemas electrónicos:

I. Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal.
II. Sistema de los servidores públicos que intervengan en procedimientos de contrataciones públicas.
III. Sistema nacional de servidores públicos y particulares sancionados.
IV. Sistema de información y comunicación del Sistema Nacional y del Sistema Nacional de Fiscalización.
V. Sistema de denuncias públicas de faltas administrativas y hechos de corrupción.
VI. Sistema de Información Pública de Contrataciones.

Adicionalmente, en términos del artículo 4 de las Bases para el funcionamiento de la PDN, la Plataforma es un instrumento de inteligencia institucional del Sistema Nacional Anticorrupción para el

cumplimiento de sus funciones, obligaciones y facultades, y está compuesta por los elementos informáticos a través de los cuales se integran y conectan los diversos sistemas, subsistemas y conjuntos de datos, que contienen datos e información relevante para ello.

Tal como se analizará de manera particular en el apartado siguiente, es posible advertir que la PDN reúne las características previstas para la procedencia de la elaboración y presentación de una Evaluación de impacto en la protección de datos personales, atendiendo a lo siguiente:

- Constituye una puesta en operación que implica un tratamiento de datos personales.
- Dicho tratamiento se realiza a través de una plataforma informática.
- La puesta en operación realizada a través de la plataforma informática de referencia implica un tratamiento relevante o intensivo.

No obstante, atendiendo los supuestos previstos por los artículos 75 y 76 de la Ley General y 8 y 9 de las Disposiciones administrativas, se advierte que, la elaboración y presentación de una Evaluación de impacto en la protección de datos personales, debe considerarse en el análisis realizado, tanto las hipótesis que constituyen un tratamiento relevante o intensivo de carácter general, así como los diversos tratamientos relevantes o intensivos de carácter particular, a fin de desarrollar los elementos a que hace referencia el artículo 14 de las Disposiciones administrativas, en congruencia con el cumplimiento de criterios relativos a la observancia de principios, deberes y derechos previstos por la Ley General y los Lineamientos generales.

En ese sentido, el objeto del presente Dictamen se encuentra relacionado con el análisis de los supuestos de tratamiento relevante o intensivo de carácter general y/o particular, para lo cual, en lo que hace al primer supuesto, es decir, respecto al tratamiento relevante o intensivo de carácter general, y, considerando que la PDN, se integra a través de 6 sistemas y diversos subsistemas, se considera importante identificar, conforme el contexto reportado por la SESNA, las características

REQUERIMIENTOS EIPDP	S1	S2	S3	S4	S5	S6
TRANSFERENCIAS	SÍ	SÍ	SÍ	SÍ	SÍ	SÍ
DATOS PERSONALES SENSIBLES	SÍ	NO	NO	NO	N/D	NO
RIESGOS	SÍ	N/D	N/D	N/D	N/D	N/D

TRATAMIENTO RELEVANTE O INTENSIVO DE CARÁCTER GENERAL	SI	N/D	N/D	N/D	N/D	N/D

Luego entonces, vale la pena señalar que tomando como referencia la información proporcionada por la SESNA, y sin prejuzgar sobre la actualización de la hipótesis de tratamiento relevante o intensivo respecto de sistemas diversos que pudieran hacer exigible dicha obligación por parte del responsable, que, el tratamiento a realizarse dentro del S1, es susceptible de considerarse tratamiento relevante o intensivo de carácter general, al reunirse las condiciones siguientes:

- Existan riesgos inherentes a los datos personales a tratar, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de titulares involucrados; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas.
- Se traten datos personales sensibles a los que se refiere el artículo 3, fracción X de la Ley General, entendidos como 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. Requerimiento que se actualiza derivado de las manifestaciones de la SESNA y del análisis del tratamiento que se realiza por parte de la información de las declaraciones de situación patrimonial.
- Se efectúen o pretendan efectuar transferencias de datos personales a las que se refiere el artículo 3 fracción XXXII de la Ley General, según corresponda, entendidas como cualquier comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado, considerando con especial énfasis, de manera enunciativa más no limitativa, las finalidades que motivan éstas y su periodicidad prevista; las categorías de titulares involucrados; la categoría y sensibilidad de los datos personales transferidos; el carácter nacional y/o internacional de los destinatarios o terceros receptores y la tecnología utilizada para la realización de éstas. Supuesto que se acredita en función de la atribución delegada que tiene la SESNA para tales efectos como administradora de la PDN.

Sin embargo, se advierte que también se actualiza un tratamiento relevante o intensivo de carácter particular, en el marco de la hipótesis señalada en el artículo 9, fracción VI, de las Disposiciones administrativas, que reconoce con tal carácter la realización de un tratamiento frecuente y continúo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.

En consecuencia, resulta importante señalar que el objeto del presente dictamen es el de llevar a cabo su análisis respecto de los tratamientos relevantes o intensivos siguientes:

- De carácter general, respecto del S1 y su interacción con otros sistemas, aplicativos y repositorios.
- De manera específica para el tratamiento relevante o intensivo de carácter particular, relativo a la realización de tratamiento frecuente y continúo de grandes volúmenes de datos personales, así como, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.

Supuestos sobre los cuales de conformidad con las hipótesis normativas previamente señaladas, correspondía a la SESNA establecer los elementos establecidos en todas las fracciones del numeral 14 de las Disposiciones administrativas en lo que hace al tratamiento relevante o intensivo de carácter general, así como, adicionalmente referir las características inherentes al tratamiento relevante o intensivo de carácter particular, debido a las notas distintivas respecto de los supuestos relativos al mencionado numeral 14, en sus fracciones III, IV y V, en torno a:

- La representación del ciclo de vida de los datos personales a tratar.
- La identificación, análisis y descripción de la gestión de los riesgos inherentes para la protección de los datos personales.
- El análisis de cumplimiento normativo en materia de protección de datos personales de conformidad con la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables.

Lo anterior, bajo la lógica prevista en las Disposiciones administrativas sobre el procedimiento establecido que implica la valoración por parte del Instituto de la Evaluación de impacto en la protección de datos personales elaborada y presentada por el sujeto obligado, la cual constituye el punto de partida y marco de referencia para poder llevar a cabo el análisis, dictaminación, y, en su caso la emisión de recomendaciones no vinculantes.

Es decir, el alcance de la revisión a realizar por parte del Instituto queda determinada en función de los elementos proporcionados por parte del sujeto obligado y del análisis que éste realizó en la Evaluación de impacto en la protección de datos personales elaborada, por lo que el Instituto no puede

sustituir o subsumir el análisis proporcionado por el propio sujeto obligado en su documento, y por ende, se encuentra circunscrito al marco de referencia provisto por el sujeto obligado.

Finalmente, es dable señalar que el trámite de la valoración de la Evaluación de impacto en la protección de datos personales se realiza en función de la información y documentación proporcionada por la entidad presentante, por lo que no resulta factible prejuzgar sobre la calidad y completitud de la información proporcionada, por lo que, las conclusiones que deriven del presente documento se encontrarán soportadas en función de lo que la SESNA reportó hacia el INAI, y en función de ello, cualquier aspecto no señalado, omitido o apreciado de manera diversa, deberá hacerse notar al Instituto a fin de brindar la clarificación correspondiente por los medios que correspondan.

En consecuencia, es posible advertir que el presente documento, se encuentra circunscrito:

- Al objeto del análisis, relativo al tratamiento relevante o intensivo de carácter general, advertido en lo que hace a la PDN sobre su sistema S1, en lo que hace a su funcionamiento e interacciones con los sistemas S2, S3, S4, S5, S6 y demás sistemas que se llegaran a desarrollar y tuvieran interacción con el mismo, por reunir los supuestos previstos por la hipótesis normativa, a saber, se identifican transferencias[12], tratamiento de datos personales sensibles[13] y riesgos inherentes a dicho manejo. Así mismo, el objeto del análisis también comprende el tratamiento relevante o intensivo de carácter particular, la realización de un tratamiento frecuente y continúo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.
- El alcance del presente documento se encuentra limitado las derivaciones lógicas que surgen del análisis de los documentos presentados por la SESNA, por lo cual, si bien el objeto del presente documento implica el análisis del tratamiento relevante o intensivo de carácter general y particular señalados en el punto previo, éste se encuentra circunscrito al análisis provisto por la SESNA en su Evaluación de impacto en la protección de datos personales, lo cual implica, que esta unidad administrativa no se encuentra en aptitud de llevar a cabo un análisis específico si este no deriva de supuestos establecidos por la SESNA en el instrumento bajo revisión.

---

[12] Sobre el particular, conviene señalar que en términos del artículo 3, fracciones XXVIII y XXXII, por responsable debe entenderse a los sujetos obligados a que se refiere el artículo 1 de la Ley General que deciden sobre el tratamiento de datos personales, y, por transferencia, toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado; es posible advertir que la existencia de transferencias que se identifica para atribuir el tratamiento relevante o intensivo es de índole normativo, puesto que se advierte que en el presente supuesto, se esta en presencia de comunicaciones de datos realizada a persona distinta del titular, del responsable o del encargado, en el entendido de que la SESNA es susceptible de considerarse como responsable del tratamiento de datos personales de la PDN, en términos de lo previsto por los artículos 48, segundo párrafo, de la Ley General del SNA, y 6, de las Bases de funcionamiento de la PDN, debido a que decide sobre dicho tratamiento en términos de las funciones atribuidas por el Comité Coordinador en dichas Bases.

[13] Definidos por la SESNA en su Evaluación de impacto en la protección de datos personales y en su documento de seguridad como tales, catalogados en función de la definición provista por el artículo 3, fracción X, de la Ley General.

- Este dictamen se emite con la salvedad de que en su elaboración se tomaron en consideración los datos, información y documentos proporcionados por la SESNA en su Evaluación de impacto en la protección de datos personales y en el requerimiento de información adicional que le hubiera sido formulado, por lo cual, no puede prejuzgarse sobre la calidad de dicha información, y por ende, cualquier precisión deberá ser requerida por parte de la entidad presentante.

V. Análisis del tratamiento de datos personales que conllevará la Plataforma Digital Nacional, respecto a los sistemas identificados como S1, S2, S3 y S6.

Como ya fue mencionado, los artículos 74 y 77 de la Ley General y 10 de las Disposiciones administrativas prevén que el responsable está obligado a elaborar y presentar una evaluación de impacto en la protección de datos personales ante el Instituto, al menos 30 días hábiles anteriores a la fecha en que pretenda poner en operación o modificar una política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que, a su juicio y de conformidad con los ordenamientos citados, implique un tratamiento intensivo o relevante de datos personales.

Al respecto, la SESNA manifestó lo siguiente:

"[...]

La Plataforma se encuentra operando en su versión Beta 0.7 y, dadas sus características como una plataforma modular y escalable, se estima que ***comenzará a realizar un tratamiento frecuente y continuo de grandes volúmenes de datos y cruces de información con múltiples sistemas informáticos posterior al mes de mayo del año 2021****, fecha límite en la que todos los servidores públicos de los tres órdenes de gobierno deben presentar sus declaraciones de situación patrimonial y de intereses en los formatos aprobados para tal efecto por el Comité Coordinador del Sistema Nacional Anticorrupción, en términos de lo ordenado por el "ACUERDO por el que el Comité Coordinador del Sistema Nacional Anticorrupción da a conocer que los formatos de declaración de situación patrimonial y de intereses son técnicamente operables con el Sistema de Evolución Patrimonial y de Declaración de Intereses de la Plataforma Digital Nacional, así como el inicio de la obligación de los servidores públicos de presentar sus respectivas declaraciones de situación patrimonial y de intereses conforme a los artículos 32 y 33 de la Ley General de Responsabilidades Administrativas", publicado en el Diario Oficial de la Federación el 24 de diciembre de 2019." (Sic)*

De las manifestaciones anteriores, el Instituto advierte que la PDN, al momento de presentar la evaluación de impacto en la protección de datos personales que nos ocupa, ya se encuentra operando en su versión Beta 0.7, versión en la que, de acuerdo con lo analizado, todavía no se lleva a cabo un

tratamiento frecuente y continuo de grandes volúmenes de datos y cruces de información con múltiples sistemas informáticos, pues la información de los diversos sistemas aún no se ven reflejados en la PDN.

Al respecto, se observa que conforme a lo señalado por la SESNA, la PDN no es una herramienta estática ya que, si bien es cierto que la Ley General del Sistema Nacional establece las bases normativas de la composición de la PDN, también lo es que dicha determinación normativa se refiere a la consolidación del piso mínimo o punto de partida de la Plataforma y que exige explícitamente la creación de mecanismos de evaluación y revisión que aseguren su evolución a partir de la identificación de necesidades de sus usuarios.

Es por ello que la PDN no puede ser vista con una visión de inmediatez y de resultado, sino como una herramienta que se mantendrá en permanente evolución de acuerdo con las necesidades propias del SNA. Por lo tanto, se indica que construcción es modular por lo que se encuentra en constante revisión y evolución.

Dadas sus características como una plataforma modular y escalable, se estima que comenzará a realizar un tratamiento frecuente y continuo de grandes volúmenes de datos y cruces de información con múltiples sistemas informáticos posterior al mes de mayo del año 2021, fecha límite en la que todos los servidores públicos de los tres órdenes de gobierno deben presentar sus declaraciones de situación patrimonial y de intereses en los formatos aprobados para tal efecto por el Comité Coordinador del Sistema Nacional Anticorrupción.

De las manifestaciones anteriores, es posible advertir que la multicitada plataforma, si bien se refiere a que se encuentra activa en su versión Beta 0.7, al momento de presentar la evaluación de impacto en la protección de datos personales que nos ocupa, no se encuentra en plena operación ya que no cuenta con la totalidad de la información necesaria en los sistemas que la integran al momento, lo cual se realizará de manera paulatina, dada su naturaleza de permanente evaluación.

Por lo cual, este Instituto determina que la PDN cumple con el requisito a que se refieren los artículos 74 y 77 de la Ley General y 10 y 23 de las Disposiciones administrativas respecto a que el responsable está obligado a elaborar y presentar una evaluación de impacto en la protección de datos personales de manera previa, esto es al menos 30 treinta días hábiles anteriores, a la puesta en operación o modificación de una política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.

Ahora bien, los artículos 75 de la Ley General y 8 de las Disposiciones administrativas establecen los supuestos que deben concurrir para considerar a un tratamiento de datos personales con la connotación general de intensivo o relevante, a saber:

- Cuando existan riesgos inherentes a los datos personales a tratar, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de titu ares; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas.
- Se traten datos personales sensibles que refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conllevar un grave riesgo 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.
- Se efectúen o pretendan efectuar transferencias de datos personales, entendidas como cualquier comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado, considerando con especial énfasis, de manera enunciativa más no limitativa, las finalidades que motivan éstas y su periodicidad prevista; las categorías de titulares; la categoría y sensibilidad de los datos personales transferidos; el carácter nacional y/o internacional de los destinatarios o terceros receptores y la tecnología utilizada para la realización de éstas.

En primer lugar, es importante advertir porque la actividad que realiza la SESNA en torno a la PDN, le atribuye el carácter de responsable en términos del artículo 1, párrafos segundo y quinto, y 3, fracción XXVIII de la Ley General, al configurarse un tratamiento de datos personales a través de la PDN.

En este sentido, debe tomarse en consideración que, en términos del artículo 3, fracción XXXIII de la Ley General, por tratamiento de datos personales se entiende 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 personales.

De conformidad con los artículos 3, 4 y 25 de las Bases para el funcionamiento de la PDN, se desprende que esta plataforma es un instrumento de inteligencia institucional y está compuesta por los elementos informáticos a través de los cuales se integran y conectan los diversos sistemas,

subsistemas y conjuntos de datos, que contienen datos e información relevante para ello. Asimismo, la PDN asegurará la interoperabilidad de la información de los diversos sistemas que se conecten e integren a la misma.

Para ello debe entenderse por la interoperabilidad a la capacidad para que sistemas y datos, puedan interactuar a través de estándares comunes, entendiendo que dicha interacción implica que las dependencias o entidades puedan compartir infraestructura, información y conocimiento mediante el intercambio de datos entre sus respectivos sistemas tecnológicos.

Ahora bien, de conformidad con lo manifestado por la SESNA, así como de lo identificado en la página oficial de la PDN, se indica que esta plataforma logrará la interoperabilidad técnica con los diversos sistemas que la integrarán a través de la creación de estándares de datos y mediante el uso de APIs. Los estándares de datos permitirán homologar la manera en que la información se debe representar para su entrega a la PDN, mientras que las APIs serán el mecanismo que permitirá la comunicación entre sistemas a través de Internet.

De lo anterior, es preciso advertir que a través de la PDN se llevará a cabo la interoperabilidad de diversos sistemas de información a fin de que, a partir de dicha interacción entre dichos sistemas, se pueda permitir el acceso a la información y datos que yace en ellos. Es decir, que a través de la PDN se facilita un canal por medio del cual es posible la interoperabilidad e interacción de los sistemas de información antes señalados, de los cuales se advierte, incluyen datos personales de personas físicas identificadas e identificables, en términos del artículo 3, fracción IX de la Ley General; a efecto de permitir que diversos usuarios pueden tener acceso y consulta a esta información a través de la plataforma, lo cual implica, un acceso de gran alcance a esta información dada la conexión con múltiples sistemas a través de la PDN.

De esta manera, la figura de tratamiento de datos personales a que se refiere el artículo 3, fracción XXXIII de la Ley General se actualiza **a partir de cualquier operación** que se realice con los datos personales. En este sentido, es indiscutible que la SESNA procesará una serie de datos personales a través de la PDN para el acceso, cruce e integración de los datos personales de los diferentes sistemas que la alimentarán, con el objeto de disponer de dicha información para su consulta y disposición en la plataforma digital; con la finalidad de permitir el manejo y aprovechamiento de los datos personales que obran en los seis sistemas; así como para la transferencia y uso de dicha información de carácter personal, por parte de las diversas autoridades competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción; acciones que, en su conjunto, constituirán un tratamiento de datos personales.

Por lo cual, para efectos del presente dictamen, el tratamiento de los datos personales que se llevará a cabo a través de la PDN por parte de la SESNA se divide en tres fases.

La primera fase del tratamiento de los datos personales está relacionada con la interacción, acceso, cruce e integración de los datos personales de diversos sistemas y bases de datos a la PDN.

La segunda fase refiere al uso, manejo y aprovechamiento que la SESNA realizará con los datos personales de los diferentes sistemas que interoperen con la plataforma, a efecto de permitir el acceso y consulta pública de la información y datos personales que obran en los seis sistemas; así como contar y proporcionar información relevante de carácter estadístico de la información de cada uno de los sistemas.

La tercera fase del tratamiento de datos personales que llevará a cabo la PDN por parte de la SESNA, corresponde al acceso, transferencia y uso de dicha información personal, en la que se incluye los datos personales de carácter confidencial, por parte de las diversas autoridades competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción.

Ahora bien, es preciso señalar que la SESNA se constituye como responsable del tratamiento que se lleve a cabo a través de la PDN toda vez que, en términos del artículo 48 de la Ley General del Sistema Nacional será quien administrará la PDN, lo cual implica proveer los servicios tecnológicos y financieros para mantener sus componentes en funcionamiento.

Asimismo, con relación a las Bases para al funcionamiento de la PDN, es posible advertir que la SESNA deberá:

- Emitir los protocolos, estándares, reglamentos, especificaciones técnicas y cualquier normativa necesaria para la colaboración, provisión de datos y acciones para cumplir con dichas Bases, los cuales serán obligatorios para todos los proveedores, concentradores y encargados a nivel federal, estatal y municipal.
- Verificar de manera permanente el correcto funcionamiento de los componentes de la Plataforma y sus sistemas, con la finalidad de prevenir fallas y, en caso de diagnosticarlas, dar pronta atención a las mismas.
- Asegurar que los usuarios tengan acceso a la Plataforma. Asimismo, vigilará y dará cuenta de su correcto funcionamiento al Comité Coordinador.
- Implementar las medidas necesarias para el cumplimiento de sus respectivas obligaciones en tiempo y forma.
- Informar bimestralmente a los integrantes del Comité Coordinador sobre el funcionamiento de la Plataforma, recomendaciones para mejorarlo, y sobre las fallas que ésta o cualquiera de

sus componentes puedan haber presentado, y las medidas que se tomarán para solucionarlas.

- Elaborar y publicar un catálogo de perfiles, en el cual se establezcan las facultades, obligaciones, y/o atribuciones que les sean aplicables a cada uno de los usuarios de manera genérica.
- Establecer los mecanismos de seguridad necesarios que garanticen la confidencialidad, integridad y disponibilidad de la información.
- Proponer y diseñar los talleres de aprendizaje en el uso de la Plataforma, y será responsable de brindar capacitación técnica y de operación de la Plataforma a los usuarios, proveedores, concentradores y encargados.
- Observar, implementar y operar los criterios generales de seguridad de la información conforme a los procesos de administración de la seguridad de la información y de operación de los controles de seguridad de la información, de conformidad con la normativa aplicable.
- Desarrollar un análisis de riesgos, que los identifique, clasifique y priorice de acuerdo con su impacto en los procesos y servicios contemplados en la Plataforma.
- Establecer un modelo de gobernanza de seguridad de la información.
- Realizar el análisis de vulnerabilidades correspondiente, el cual preferentemente será realizado por un tercero, distinto a quien desarrolló la Plataforma.
- Implementar un proceso de fortalecimiento de la seguridad de la información, así como de mejora continua sobre los controles de seguridad de la información.

Por lo anterior, tomando en consideración lo establecido en el artículo 3, fracción XXVIII la SESNA se constituye como responsable del tratamiento de datos personales, en primera instancia, debido a que, como administradora de la PDN, tiene la decisión de determinar los servicios tecnológicos y financieros que permitan el funcionamiento de la plataforma, es decir, que permitan la principal funcionalidad de la plataforma que es la integración y conexión de los datos personales que yacen en los diversos sistemas con la PDN, y a su vez su acceso y consulta.

En este sentido, la SESNA será quien emita, por ejemplo, las especificaciones técnicas sobre los campos mínimos de datos que debe contener cada sistema, así como los estándares que deben seguir cada campo para ser interoperables con la PDN a efecto de que, a partir de este orden de los datos, se pueda llevar a cabo su acceso y consulta en la PDN. De igual forma, decidirá el formato de especificación mediante el cual se den las características con las que deberán contar las APIs que integrarán la PDN y que permitirán la comunicación entre sistemas a través de Internet.

Asimismo, la SESNA también deberá verificar de manera permanente el correcto funcionamiento de los componentes de la Plataforma y sus sistemas, con la finalidad de prevenir fallas y, en caso de diagnosticarlas y dar pronta atención a las mismas, así como implementar mecanismos de seguridad

necesarios que garanticen la confidencialidad, integridad y disponibilidad de la información, realizar el análisis de riesgos y vulnerabilidades en torno a los procesos y servicios de la PDN, así como establecer y regular el acceso que se realice a la información que podrá ser consultable a través de la plataforma.

De esta manera, se concluye que la SESNA será responsable del tratamiento de datos personales en términos de lo dispuesto en el artículo 3, fracción XXVIII al decidir sobre los mecanismos y medios tecnológicos mediante los cuales se dará el acceso, cruce e integración de los datos personales de los diferentes sistemas que la alimentarán, asimismo establecerá las pautas para la consulta y disposición en la plataforma digital de dichos datos; aunado a que establecerá los mecanismos y reglas para permitir la transferencia y uso de datos personales, por parte de las diversas autoridades competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción; acciones que, en su conjunto, constituyen un tratamiento de datos personales.

Ahora bien, con relación al primer requisito para considerar que cierto tratamiento de datos personales tiene la connotación de relevante o intensivo en términos de los artículos 75, fracción I de la Ley General y 8, fracción I de las Disposiciones administrativas, es decir, cuando existan riesgos inherentes a los datos personales, conviene señalar que en todo tratamiento de datos personales siempre existirán riesgos por el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de titulares; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas.

Tan es así, que conforme a los artículos 31 y 32 de la Ley General y 55 y 60 de los Lineamientos Generales el responsable está obligado a implementar y mantener medidas de seguridad de carácter físico, técnico y administrativo que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, considerando los riesgos inherentes y asociados a los datos personales.

Para lo cual, el responsable está obligado a llevar a cabo un análisis de riesgos de los datos personales tratados considerando los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; el valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida; el valor y exposición de los activos involucrados en el tratamiento de los datos personales; las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida; la sensibilidad de los datos personales; el desarrollo tecnológico; las posibles consecuencias de una vulneración para los titulares; las trasferencias de datos personales que se realicen; el número de titulares; las vulneraciones previas ocurridas, entre otros factores.

Al respecto, conviene señalar que la SESNA indicó lo siguiente:

> *"[...]*
>
> ***Riesgos detectados***
>
> *Es fundamental destacar que la PDN es una plataforma de interoperabilidad, y como lo establece la normatividad vigente (Bases de la PDN, LGRA, LGSNA), los Encargados son los responsables de recibir, ordenar y/o resguardar los datos e información en los subsistemas para su integración a los sistemas de la PDN.*
>
> - ***Incumplimiento de los Protocolos y normas de seguridad:*** *Es responsabilidad de los Encargados cumplir con todos los protocolos de seguridad emitidos y recomendados por la USTPDN para el tratamiento y transferencia de los datos. En caso de no cumplir con los protocolos y de darse una vulnerabilidad en términos de los datos y/o en el proceso de su transmisión, los Encargados deberán responder y realizar los ajustes necesarios para garantizar la seguridad de la información.*
> - ***Mal uso de los datos:*** *sucede cuando un servidor público con facultades para acceder a información pública o clasificada transgrede los términos y condiciones de la PDN o las obligaciones contenidas en la LGPDPPSO.*
> - ***Información inexacta y/o equivocada:*** *Cuando los Encargados transfieren a la PDN información inexacta, campos adicionales, datos reservados y otro tipo de información que por sus características no debe ser pública o parte de la PDN.*
> - ***Acceso no autorizado:*** *En el caso en el que se identifique o reporte un acceso a la PDN que caiga en alguno(s) de los siguientes supuestos: acceso sin autorización, contra derecho, habiendo obtenido de manera ilegal claves de acceso a un sistema con información reservada.*
> - ***Robo de dispositivos de infraestructura:*** *Dispositivos de almacenamiento o equipo de cómputo en los que se encuentre información sensible sobre la arquitectura o desarrollo de la PDN, configuraciones y otros datos que pudieran ser utilizados para acceder, transgredir o modificar la PDN y su contenido." (Sic)*

De lo anterior, el Instituto advierte que en el tratamiento de los datos personales que se llevará a cabo respecto de los seis sistemas que la conformarán, el responsable identificó una serie de riesgos a los que podrían estar expuestos los datos personales.

Ahora bien, en el documento de seguridad adjunto a la evaluación de impacto en la protección de datos personales que nos ocupa, resulta relevante indicar que la SESNA señaló el nivel de riesgo de los datos personales que serán tratados a través de la PDN, al respecto, se puede advertir que:

- La información que se podrá consultar a través del S1 es de alto riesgo dados los diferentes tipos de datos que se podrán consultar en el sistema, pues no sólo se tendrán datos de identificación de la persona servidora pública, su pareja y dependientes económicos, sino también datos relacionados con su patrimonio además de que, con la información presentada

en la declaración de intereses, se indica que se podría inferir datos personales relativos a creencias religiosas, filosóficas, morales, afiliación sindical u opiniones políticas. El nivel de alto riesgo también se atribuye debido al volumen de los datos a tratar, toda vez que, una vez que todos los sujetos obligados desarrollen las herramientas informáticas para conectarse a la PDN, se podrá consultar la información de 6 millones de personas servidoras públicas de todos los niveles de gobierno y órganos autónomos.

- Con respecto de los datos personales de los S2, S3 y S6, se estipulan de riesgo inherente bajo ya que únicamente contiene datos de identificación de las personas servidoras públicas sancionados y cue intervienen en procedimientos de contrataciones públicas, así como proveedores. Asimismo, se indica que el volumen de titulares irá incrementando ya que depende de los procedimientos de contrataciones públicas y sancionadores que se realicen, los cuales forman parte de las funciones primordiales del Estado. Al unir estos dos valores se concluyó que el nivel de riesgo es 1, el más bajo en la metodología.

En ese sentido, si bien la SESNA no refiere la probabilidad con la que se podrían presentar tales riesgos, ni acredita un análisis particular en función de la estructura asociada a la plataforma informática, es evidente que en todo tratamiento de datos personales implica diversos riesgos, que con independencia de su consideración o no para su administración, deben ser identificados y monitoreados considerando las modificaciones del contexto del tratamiento al que está sujeta, sobre todo si consideramos que la PDN actualiza la realización de un tratamiento frecuente y continúo de grandes volúmenes de datos personales y lleva a cabo cruces de información con múltiples sistemas o plataformas informáticas; hipótesis que, como más adelante se indicará debería considerar en el marco del artículo 32 de la Ley General, lo siguiente:

- 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.
- 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.

En razón de lo anterior, el Instituto determina que el tratamiento de datos personales que conllevará la implementación de la PDN respecto de la integración e interoperabilidad respecto de los seis sistemas que la conformarán, actualiza la primera condición para considerar a un tratamiento de datos personales con el carácter de intensivo o relevante prevista en los artículos 75, fracción I de la Ley

General y 8, fracción I de las Disposiciones administrativas, esto es, la existencia de riesgos inherentes a los datos personales a tratar, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso.

Respecto al segundo requerimiento para considerar que se está en presencia de un tratamiento relevante o intensivo de datos personales conforme a los artículos 75, fracción II de la Ley General y 8, fracción II de las Disposiciones administrativas, es decir, la utilización de datos personales de carácter sensible, la SESNA manifestó lo siguiente:

> *"[...]*
> ***II. INFORMACIÓN DEL SISTEMA S1***
> *[...]*
> ***II. 4. Tipo de datos personales, precisando los datos personales sensibles.***
> *[...]*
> ***En este último acuerdo, se especifican todos los datos personales que se tratan en el S1, así como aquellos que son públicos, reservados o confidenciales,*** incluyendo los datos personales sensibles, entre los que se encuentran los datos patrimoniales del declarante, su cónyuge, hijos y dependientes económicos *bajo los siguientes rubros:*
> *1. Ingresos netos del declarante;*
> *2. Bienes Inmuebles;*
> *3. Bienes muebles;*
> *4. Inversiones, Cuentas Bancarias y otro tipo de Valores/Activos;*
> *5. Adeudos/Pasivos del declarante;*
> *6. Participación en empresas, sociedades, asociaciones;*
> *7. Apoyos o beneficios públicos;*
> *8. Beneficios privados, y*
> *9. Fideicomisos.*
>
> *Para determinar la clasificación de estos datos es importante reiterar que algunos de los datos contenidos en el S1 pertenecen a personas que no son servidoras públicas por lo que no están sujetos al mismo régimen de rendición de cuentas y transparencia.*
>
> *En sentido estricto, los datos sensibles se refieren "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 acuerdo con los datos enlistados, la información contenida en los numerales 6, 7, 8 y 9 se califican como sensibles ya que podrían revelar información respecto de las creencias religiosas, filosóficas u opiniones políticas de sus titulares. Los datos contenidos en los demás numerales podrían clasificarse como patrimoniales. Sin embargo, se propone interpretar el contenido de la información en su conjunto, especialmente porque el formato en el que serán capturados y a través del cual se tendrá acceso a la información no permite distinguir entre numerales.***
>
> *Al hacer un análisis integral de la información contenida en el S1* ***se considera que los patrimoniales también deben ser considerados como sensibles ya que en conjunto con la totalidad de información contenida en el S1, un acceso no autorizado, podría poner en riesgo la integridad del titular****."*

Documento de seguridad
"Sistema de Tratamiento de Datos Personales del Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal (en lo sucesivo, S1).

Datos personales contenidos en el sistema:
[…]

Nivel Sensible		
Tipo de Datos Personales	*Documentos*	*Datos Personales*
Datos de identificación de la pareja y dependientes económicos del declarante.	- Formatos de declaraciones: de situación patrimonial y de intereses	- Nombre - RFC - Estado civil o parentesco con el declarante - Lugar de nacimiento - Fecha de nacimiento - Nacionalidad - Domicilio
Datos de patrimoniales de la pareja o dependientes económicos del declarante	- Formatos de declaraciones: de situación patrimonial y de intereses	- Ingresos netos - Bienes Inmuebles - Bienes muebles - Inversiones, cuentas Bancarias y otro tipo de Valores, Activos - Adeudos/Pasivos - Participación en empresas, sociedades, asociaciones - Apoyos o beneficios públicos - Beneficios privados - Fideicomisos

[…]" (Sic)

Aunado a lo anterior, en la respuesta al requerimiento de información, la SESNA manifestó lo siguiente:

"4. Como se explicó en la Evaluación, el componente privado del Sistema 1 incluirá información del declarante, cónyuge, hijos y dependientes económicos respecto de:

- *Su participación en empresas, sociedades y asociaciones.*
- *Apoyos o beneficios públicos que reciben.*
- *Beneficios privados.*
1. *Fideicomisos de los que son parte.*

*Esta información podría revelar información respecto de las creencias religiosas, filosóficas u opiniones políticas de sus titulares. Por ejemplo, si forma parte de alguna asociación religiosa. **Esto no significa que en todos los casos contenga información sensible pero ante la posibilidad se propone clasificarlos como sensibles**." (Sic)*

[Énfasis añadido]

Ahora bien, como ya fue señalado, la PDN estará integrando diversos sistemas, en los cuales se desprende contienen datos de carácter personal, al referir información concerniente a una persona física identificada o identificable, en términos de lo dispuesto en el artículo 3, fracción IX, de la Ley General.

En tal virtud, en relación con la actualización sobre la fracción II del artículo IX de las Disposiciones administrativas, esto es que se configure el tratamiento de datos personales de carácter sensible, específicamente por lo que hace al S1, se observa que los datos personales contenidos en el mismo son los siguientes:

S1. Formatos de las declaraciones de situación patrimonial y de intereses:

Datos del declarante:

- Nombre.
- Primer y segundo apellido.
- Clave Única de Registro de Población (CURP).
- Registro Federal de Contribuyentes (RFC) y homoclave.
- Correo electrónico institucional.
- Correo electrónico personal/alterno.
- Número telefónico de casa.
- Número celular personal.
- Régimen matrimonial.
- Estado Civil.
- País de nacimiento.
- Fecha de nacimiento.
- Nacionalidad.
- Firma.
- Domicilio.
- Escolaridad (último grado de estudios).
- Institución educativa donde se realizaron los estudios.
- Lugar donde se ubica la institución educativa.
- Carrera o área de conocimiento.
- Estatus.
- Fecha de obtención del documento.
- Documento obtenido.
- Empleo/cargo/comisión.

- Nivel del empleo, cargo o comisión.
- Función o actividad principal que desempeña en su empleo, cargo o comisión.
- Fecha de toma de posesión/conclusión del empleo, cargo o comisión.
- Nombre del ente público al cual se encuentra adscrita la plaza.
- Área de adscripción.
- Ámbito público.
- Nivel/orden de gobierno.
- Teléfono de oficina y extensión.
- Domicilio del empleo, cargo o comisión.
- Experiencia laboral.
- Años laborados.
- Ámbito/sector en el que se laboró.
- Ingresos netos del declarante.
- Bienes inmuebles.
- Vehículos.
- Bienes muebles.
- Inversiones.
- Cuentas bancarias.
- Otro tipo de valores/activos.
- Adeudos/pasivos.
- Préstamo o comodato por terceros.
- Participación en empresas, sociedades, asociaciones.
- Apoyos o beneficios públicos.
- Beneficios privados.
- Fideicomisos.
- Representación.

Datos del cónyuge del declarante:

- Nombre.
- Primer y segundo apellidos.
- CURP.
- RFC y homoclave.
- Relación con el Declarante.
- Estado civil.
- Lugar de nacimiento.
- Fecha de nacimiento.

- Nacionalidad.
- Lugar de residencia.
- Domicilio.
- Actividad laboral.
- Lugar de trabajo.
- Ingresos netos.
- Otros ingresos.
- Bienes inmuebles.
- Vehículos.
- Bienes muebles.
- Inversiones, cuentas bancarias u otro tipo de valores /activos.
- Adeudos/pasivos.
- Préstamo o comodato por terceros.
- Participación en empresas, sociedades, asociaciones.
- Apoyos o beneficios públicos.
- Beneficiarios privados.
- Fideicomisos.
- Representación.

Datos de los dependientes económicos del declarante:

- Nombre completo.
- Primer y segundo apellidos.
- CURP.
- RFC y homoclave.
- Parentesco con el declarante.
- Lugar de nacimiento.
- Fecha de nacimiento.
- Nacionalidad.
- Lugar de residencia.
- Domicilio.
- Actividad laboral.
- Lugar de trabajo.
- Ingresos netos.
- Otros ingresos.
- Bienes inmuebles.
- Vehículos.

- Bienes muebles.
- Inversiones, cuentas bancarias u otro tipo de valores /activos.
- Adeudos/pasivos
- Préstamo o comodato por terceros.
- Participación en empresas, sociedades, asociaciones.
- Apoyos o beneficios públicos.
- Beneficiarios privados.
- Fideicomisos.
- Representación.

Datos de los clientes principales del servidor público/pareja/dependiente económico:

- Nombre completo.
- RFC.
- Sector productivo al que pertenece.
- Servicio que proporciona.
- Lugar donde se ubica.

Datos de terceros relacionados con el declarante:

- Nombre completo.
- RFC.
- Dato que permita su identificación.
- Relación del transmisor del vehículo con el titular.
- Relación del transmisor de la propiedad con el titular.
- Relación con el dueño o titular.

Datos de servidores públicos que intervienen en procedimientos de contrataciones públicas:

- Nombre completo del servidor público.
- Nombre completo de la persona servidora pública que funge como superior jerárquico.
- RFC del servidor público.
- CURP del servidor público.
- RFC de la persona servidora pública que funge como superior jerárquico.
- CURP persona servidora pública que funge como superior jerárquico.

Datos de particulares, personas físicas y morales, que se encuentren inhabilitados para celebrar contratos con entes públicos:

- Nombre.
- RFC.

- Tipo de falta.
- Causas, motivos o hechos de sanción.

Datos personales de servidor público sancionado:

- Nombre del servidor público sancionado.
- Género servidor público sancionado.
- RFC servidor público sancionado.
- CURP servidor público sancionado.
- Dependencia.
- Tipo de falta.
- Causas, motivos o hechos de la sanción.
- Tipo de sanción.

Datos personales de particulares sancionados:

- Nombre del particular sancionado.
- RFC del particular sancionado.
- Dependencia.
- Tipo de falta.
- Causas, motivos o hechos de la sanción.
- Tipo de sanción.

Datos personales de servidores públicos y particulares que intervienen y participan en los procedimientos de contrataciones públicas, y personas físicas a las que se les adjudica un contrato público:

- Nombre de las personas servidoras públicas que intervienen en los procedimientos de contrataciones públicas.
- Nombre de las personas físicas que participan en procedimientos de contrataciones públicas.
- Nombre de las personas físicas a las que se las adjudica un contrato público.

Al respecto, cabe señalar que el anterior listado se refiere conforme a lo manifestado por la SESNA en la evaluación de impacto presentada. No obstante, este Instituto advierte que el contenido de los datos personales que conforman el Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal, identificado anteriormente para efectos del presente

Dictamen como S1, se encuentran expresamente contenidos en los formatos de situación patrimonial y de intereses[14], publicados por el Comité Coordinador del SNA.

En este sentido, conviene señalar que el **artículo 3, fracción X** de la Ley General de Datos prevé como datos personales sensibles:

> *"**Artículo 3.** Para los efectos de la presente Ley se entenderá por:*
>
> *[...]*
>
> *I. **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;*
>
> *[...]" (Sic)*

Por lo anterior, se puede determinar que un dato personal adquiere categoría de sensible en cualquiera de los siguientes supuestos:

a. Que se refieran a la esfera más íntima de su titular.
b. Que su utilización indebida pueda dar origen a discriminación.
c. Que su utilización indebida conlleve un riesgo grave para su titular.
d. Datos personales que puedan revelar aspectos como origen racial o étnico.
e. Datos personales que puedan revelar aspectos como estado de salud presente o futuro.
f. Datos personales que puedan revelar aspectos como información genética.
g. Datos personales que puedan revelar aspectos como creencias religiosas, filosóficas y morales.
h. Datos personales que puedan revelar aspectos como opiniones políticas.
i. Datos personales que puedan revelar aspectos como preferencia sexual.

Es de precisar que la Ley General establece una lista enunciativa más no limitativa de este tipo de datos personales, lo cual no excluye que en atención del contexto y de las circunstancias particulares de cierto tratamiento, un dato personal pueda ser considerado como sensible partiendo de la premisa que éstos podrían afectar la esfera más íntima de su titular o cuya utilización indebida podría dar origen a discriminación o conllevar un grave riesgo para éste.

---

[14] Publicados en el DOF 23 de septiembre de 2019, y su modificación publicada en el DOF el 23 de septiembre 2019, disponibles en los siguientes vínculos electrónicos: http://dof.gob.mx/nota_detalle.php?codigo=5573194&fecha=23/09/2019 y https://dof.gob.mx/nota_detalle.php?codigo=5544152&fecha=16/12/2019, consultados por última vez el 18/05/2021

En este sentido, corresponde al sujeto obligado determinar los casos en donde dicha información es sensible pues no se excluye que en atención del contexto y de las circunstancias particulares de cierto tratamiento, un dato personal pueda ser considerado como sensible partiendo de la premisa que éstos podrían afectar la esfera más intima de su titular o cuya utilización indebida podría dar origen a discriminación o conllevar un grave riesgo para éste.

De esta manera, hacer referencia al tratamiento de datos personales sensibles implica una categoría especial de tratamiento que comprende diversos supuestos que en el ámbito de sujetos obligados son enunciativos, es decir, que no se limitan a los supuestos determinados de manera expresa en dicha disposición.

Ahora bien, es preciso señalar que, del listado de datos personales previamente señalado, es posible advertir que por lo que refiere a los datos personales del S1 respecto de los datos que obran en el formato de declaración patrimoniales y de intereses, pueden configurar datos personales de carácter sensible.

Lo anterior, ya que, en principio, del contenido de los formatos en comento, podrían advertirse como datos personales sensibles aquéllos que pudieran estar relacionados con la pertenencia del declarante, cónyuge, concubina o concubinario y/o dependientes económicos del declarante o terceros, referentes a:

- Asociaciones y membresías relacionadas con creencias religiosas, filosóficas y morales y
- opiniones políticas.
- Membresías relacionadas con temas de salud o preferencia sexual.
- Apoyos públicos o beneficios relacionados con cuestiones de salud, preferencia sexual o incluso origen racial o étnico.

Lo cual, de ninguna manera impide que cualquier otro dato personal contenido en los formatos para la declaración patrimonial y de intereses pueda ser considerado como sensible en la medida que afecte la esfera más íntima del declarante, cónyuge, concubina o concubinario y/o dependientes o terceros o cuya utilización indebida pueda dar origen a discriminación o conllevar un riesgo grave para este.

En virtud de lo anterior, este Instituto determina que el tratamiento de datos personales que la PDN realiza**, por lo que hace a la integración e interoperabilidad del S1,** actualiza la segunda condición para considerar a dicho tratamiento con la connotación de intensivo o relevante a que se refieren los artículos 75, fracción II de la Ley General y 8, fracción II de las Disposiciones administrativas, esto es, la utilización de datos personales de carácter sensible, por lo que refiere como ya se dijo, en un primer

momento a los datos personales contenidos en el S1, toda vez que, el resto de los sistemas que conforman la PDN, no se advierten datos personales susceptibles de considerarse sensibles, sin menoscabo de que en atención del contexto y de las circunstancias particulares de cierto tratamiento, pudieran configurarse como tales, como podría ser el supuesto de los datos personales contenidos en el S3.

En lo que respecta a la tercera condición para considerar a un tratamiento de datos personales como intensivo o relevante prevista en los artículos 75, fracción III de la Ley General y 8, fracción III de las Disposiciones administrativas, esto es, la realización de transferencias de datos personales, la SESNA señaló lo siguiente:

"[...]

II.6 Transferencias

Tomando en cuenta que por "transferencia" se debe entender toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado,13 se manifiesta que la información contenida en el S1 es susceptible de ser transferida a las diversas autoridades de los tres órdenes de gobierno, competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción, entre las que se encuentran el Ministerio Público, órganos jurisdiccionales como el Tribunal Federal de Justicia Administrativa y sus homólogos en las entidades federativas, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras a las que alude la LGRA, como la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos.

[...]

III.6 Transferencias

No aplica.

Lo anterior, en virtud de que el S2 es solo un sistema de consulta para las diversas autoridades de los tres órdenes de gobierno, competentes en la prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.

[...]

IV.6 Transferencias

No aplica.

En virtud de que el S3 es solo un sistema de consulta para los Entes públicos del Estado mexicano que pretendan realizar un nombramiento, designación o contratación.

V.6 Transferencias

No aplica.

Lo anterior, en virtud de que el S6 es solo un sistema de consulta tanto para Entes públicos como ciudadanía en general, para facilitar la prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos." [...]"

Documento de seguridad

> *"Además, la información contenida en el S1 es susceptible de ser transferida a las diversas autoridades de los tres órdenes de gobierno, competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción, entre las que se encuentran el Ministerio Público, órganos jurisdiccionales como el Tribunal Federal de Justicia Administrativa y sus homólogos en las entidades federativas, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras a las que alude la LGRA, como la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos." (Sic)*

Asimismo, en la respuesta al requerimiento de información se señala lo siguiente:

> **"8.** *Como se señaló en la Evaluación, la información contenida en el S1 es susceptible de ser transferida a las diversas autoridades de los tres órdenes de gobierno, competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción, entre las que se encuentran el Ministerio Público, órganos jurisdiccionales como el Tribunal Federal de Justicia Administrativa y sus homólogos en las entidades federativas, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras a las que alude la LGRA, como la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos." (Sic)*

Al respecto, la SESNA manifestó que la información contenida en el S1 es susceptible de ser transferida a las diversas autoridades de los tres órdenes de gobierno, competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción, entre las que se encuentran el Ministerio Público, órganos jurisdiccionales como el Tribunal Federal de Justicia Administrativa y sus homólogos en las entidades federativas, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras a las que alude la Ley General de Responsabilidades, como la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los OIC de los Entes públicos.

Por lo que refiere al resto de los sistemas que conformarán la PDN, atendiendo a lo señalado por el SESNA se advierte que, por el momento, no se llevarán a cabo transferencias.

Al respecto, por lo que se refiere al S1, el artículo 28 de la Ley General de Responsabilidades establece que la información relacionada con las declaraciones de situación patrimonial y de intereses, podrá ser solicitada y utilizada por el Ministerio Público, los Tribunales o las autoridades judiciales en el ejercicio de sus respectivas atribuciones, el Servidor Público interesado o bien, cuando las Autoridades investigadoras, substanciadoras o resolutoras lo requieran con motivo de la investigación o la resolución de procedimientos de responsabilidades administrativas.

En este sentido el artículo 42 de las Bases para el funcionamiento de la PDN, dispone que la SESNA deberá establecer los mecanismos para que la información de dicho sistema sea solicitada y utilizada de acuerdo con las necesidades de las autoridades competentes antes mencionadas, en el ejercicio

de sus respectivas atribuciones y de conformidad con la normativa aplicable, previa aprobación del Comité Coordinador.

De lo anterior, se identifica que, para cumplir con la solicitud de dichas autoridades competentes y en su caso, puedan ser utilizadas en el ejercicio de sus respectivas atribuciones, la SESNA, como administradora del funcionamiento de esta plataforma, deberá establecer mecanismos que permitan la posibilidad de transferir dicha información a las autoridades competentes, antes referidas, con el con el objetivo de ser utilizadas para investigar y sancionar posibles faltas administrativas o delitos de corrupción, lo cual actualizará una comunicación a estas autoridades de las declaraciones patrimoniales y de intereses.

De esta manera, se advierte que se actualizarían transferencias de datos personales contenidos en el S1, entendida como toda comunicación de datos personales, dentro o fuera de territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado, de conformidad con lo establecido en el artículo 3, fracción XXXII, de la Ley General.

Conforme a lo anterior y con base en las manifestaciones de la SESNA, el Instituto cuenta con elementos para determinar que el tratamiento de datos personales que se efectuará con la implementación de la PDN por lo que hace al ***Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal*** tiene carácter de tratamiento intensivo o relevante general, en la hipótesis prevista en los artículos 75 de la Ley General y 8 de las Disposiciones administrativas.

En otras palabras, la determinación de un tratamiento intensivo o relevante de carácter general conlleva forzosamente el cumplimiento de tres condiciones, la existencia de riesgos inherentes a los datos personales tratados; el tratamiento de datos personales sensibles y la realización de transferencias de datos personales, que en el caso del tratamiento de datos personales que se realiza respecto del S1 en la PDN, se actualizan las tres condiciones, es decir:

- La existencia de riesgos inherentes a los datos personales que serán tratados, el carácter sensible de los datos personales y la pretensión de efectuar transferencias de datos personales a las que se refiere el artículo 3, fracción XXXII de la Ley General; previstas en los artículos 75, fracciones I, II y III de la Ley General y 8, fracciones I, II y III de las Disposiciones administrativas.
- Se tratan datos personales sensibles a los que se refiere el artículo 3, fracción X de la Ley General de Datos.
- Se pretende efectuar transferencias de datos personales a las que se refiere el artículo 3, fracción XXXII de la Ley General de Datos.

Supuesto que en el presente caso cobra aplicación, no obstante, conviene señalar que, no pasa desapercibido que en términos del artículo 4 de las Bases para el funcionamiento de la PDN previenen que la PDN es un instrumento de inteligencia institucional del Sistema Nacional Anticorrupción para el cumplimiento de sus funciones, obligaciones y facultades, y está compuesta por los elementos informáticos a través de los cuales se integran y conectan los diversos sistemas, subsistemas y conjuntos de datos, que contienen datos e información relevante para ello.

Por tanto, es importante advertir que la funcionalidad relativa a consultas de información solamente representa una etapa en la funcionalidad completa de la PDN, lo cual debe ser considerado con la SESNA en el marco de su sistema de gestión al que hace referencia el artículo 34 de la Ley General en función del tratamiento de datos personales que pudiera implicar.

Por otra parte, continuando con los elementos que se tienen a la vista para la emisión del presente dictamen, los artículos 76 de la Ley General y 9 de las Disposiciones administrativas señalan, de manera enunciativa más no limitativa, una serie de tratamientos intensivos o relevantes de datos personales de manera particular, mismos que se actualizan cuando ocurra alguno de los siguientes supuestos:

- Cambiar la o las finalidades que justificaron el origen de determinado tratamiento de datos personales, de tal manera que pudiera presentarse una incompatibilidad entre las finalidades de origen con las nuevas finalidades, al ser estas últimas más intrusivas para los titulares.
- Evaluar, monitorear, predecir, describir, clasificar o categorizar la conducta o aspectos análogos de los titulares, a través de la elaboración de perfiles determinados para cualquier finalidad, destinados a producir efectos jurídicos que los vinculen o afecten de manera significativa, especialmente, cuando a partir de dicho tratamiento se establezcan o pudieran establecerse diferencias de trato o un trato discriminatorio económico, social, político, racial, sexual o de cualquier otro tipo que pudiera afectar la dignidad o integridad personal de los titulares.
- Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa más no limitativa, a su edad; género; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica.
- Crear bases de datos respecto de un número elevado de titulares de tal manera que se produzca una acumulación no intencional de una gran cantidad de datos personales respecto de los mismos.
- Incluir o agregar nuevas categorías de datos personales a las bases de datos ya existentes y en posesión del responsable, de tal forma que, en caso de presentarse una vulneración a la seguridad pudiera derivarse una afectación a la esfera personal de los titulares.

- Realizar un tratamiento frecuente y continuo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.
- Utilizar tecnologías con sistemas de vigilancia; aeronaves o aparatos no tripulados; minería de datos; biometría; Internet de las cosas; geolocalización; técnicas analíticas; radiofrecuencia o cualquier otra que pueda desarrollarse en el futuro y que implique un tratamiento de datos personales a gran escala.
- Realizar transferencias internacionales de datos personales a países que no cuenten en su derecho interno con garantías suficientes y equivalentes para asegurar la debida protección de los datos personales, conforme al sistema jurídico mexicano en la materia.
- Revertir la disociación de datos personales para la consecución de finalidades determinadas, especialmente si éstas son de carácter intrusivo o invasivo al titular, entre otros.

Lo anterior, atendiendo a lo dispuesto en el artículo 76 de la Ley General. Es por ello, que cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que, a su juicio y de conformidad con la Ley General y las Disposiciones administrativas, impliquen un tratamiento intensivo o relevante específico de datos personales, está obligado a presentar una evaluación de impacto en la protección de datos personales ante el Instituto.

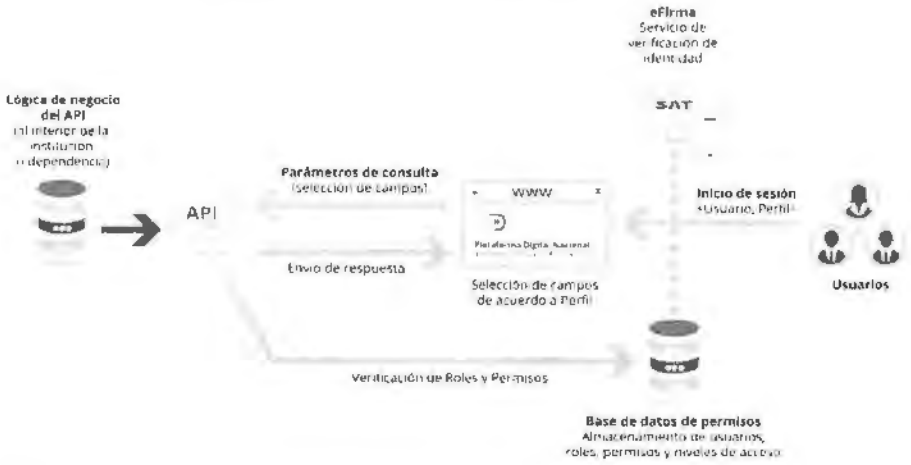
En el caso que nos ocupa, conviene traer a colación lo dispuesto en los artículos 76 de la Ley General y 9, fracción VI de las Disposiciones administrativas, es decir, se entenderá que el responsable está en presencia de un tratamiento intensivo o relevante de datos personales, de manera particular, cuando pretenda realizar un tratamiento frecuente y continúo de grandes volúmenes de datos personales, o bien, llevar a **cabo cruces de información con múltiples sistemas o plataformas informáticas.**

En relación con lo anterior, respecto al **segundo extremo** de la fracción VI del artículo 9 de las Disposiciones administrativas, esto es por lo que hace a llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas, es preciso reiterar que el tratamiento de datos personales que se lleva a cabo a través de la PDN responde a tres principales fases, haciendo en este caso, alusión a la primera, relacionada con la interacción, acceso, cruce e integración de los datos personales de diversos sistemas y bases de datos a la PDN.

La PDN como plataforma de interoperabilidad, permite esta interacción entre múltiples sistemas y bases de datos que se conectarán y alimentarán a la PDN a través del cumplimiento de determinadas especificaciones técnicas y estándares de datos que la SESNA se encuentra obligada a determinar para lograr esta interacción entre sistemas y a su vez puede ser consultada en la propia plataforma.

Para ello, cada sistema contará con su respectivo modelo estándar para la interoperabilidad que se deberán de adoptar por los sistemas proveedores de la información de la PDN, asimismo deberán adoptar el formato de especificación que permita describir de manera precisa las características con las que deberán contar las APIs para interacción entre los sistemas con la PDN.

Al respecto, y con el objetivo de contar con mayores elementos a efectos de emitir el presente dictamen, este Instituto pudo advertir en el contenido de las Especificaciones técnicas[15] para la interoperabilidad de los sistemas que conformarán la PDN, alojadas en la página de internet de la plataforma; el siguiente esquema conceptual del flujo de comunicación entre los sistemas de las instituciones y la PDN. De derecha a izquierda se observan usuarios con diferentes perfiles accediendo a la PDN y solicitando información de acuerdo con sus atribuciones:



De manera adicional, es importante referir a lo estipulado en el Análisis para la implementación y operación de la PDN, en el cual la SESNA realiza una descripción de los distintos sistemas de los proveedores de información, los cuales constituirán las fuentes de información que alimentarán a la PDN y que estarán disponibles para su consulta mediante la misma, donde al respecto se señala lo siguiente:

> *"Es importante resaltar que la PDN es el centro de una conexión que se debe realizar desde cada uno de sus seis sistemas con los conjuntos de datos de las entidades públicas que hay tanto a nivel federal como a nivel local. Es decir, los sistemas se deben conectar con un ecosistema federal, dentro del cual se encontrarán los datos generados por los Poderes Ejecutivo, Legislativo y Judicial, por los Órganos Constitucionalmente Autónomos, así como por las Empresas Productivas del Estado, y por cualquier otra*

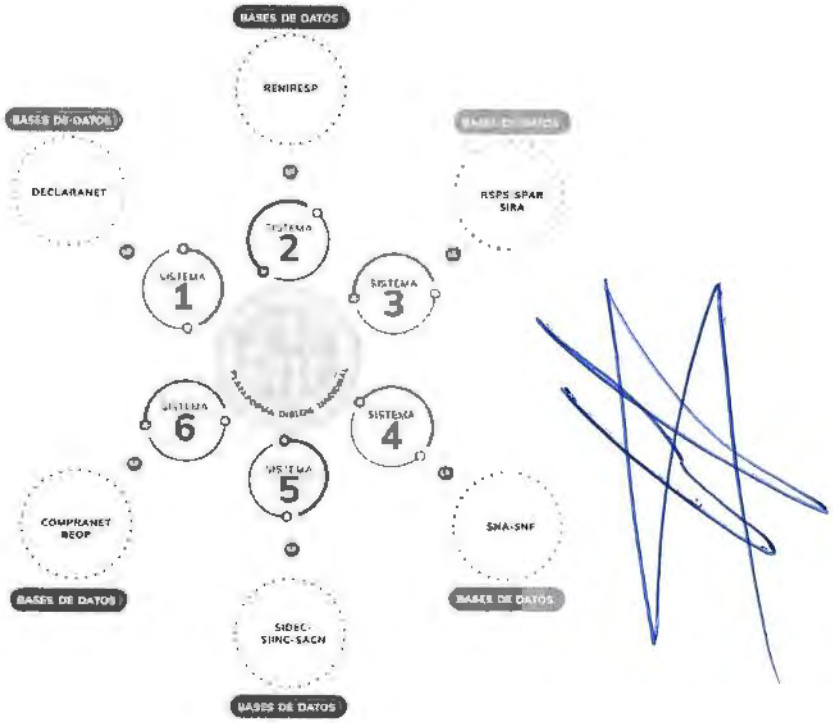
[15] Disponible en el siguiente vínculo electrónico: https://www.plataformadigitalnacional.org/especificaciones consultado por última vez el 18/05/2021.

entidad con naturaleza diferente a éstas que opere a nivel federal; sin embargo, simultáneamente, cada uno de los sistemas de la PDN deberá conectarse con los conjuntos de datos que hay en cada una de las 32 Entidades Federativas, que en términos generales, serán un espejo de la información generada a nivel federal para cada estado. Se deberá contemplar que cada Sistema Local Anticorrupción deberá contar con ese espejo de la Plataforma que contenga la información que se genera en cada Entidad Federativa, y que, a través de cada Secretaría Ejecutiva de los Sistemas Locales, se concentrará y conectará la información con la PDN.

A continuación, se muestra un ejemplo de arquitectura interna de la PDN, el cual contempla una plataforma central que está conformada por (al menos) seis sistemas de información, mismos que estarían conectados a diversas bases de datos y otros sistemas de información, tanto federales como estatales, a través de lógicas de intercambio de información (LII) (Middleware).

1. LA ARQUITECTURA INTERNA DE LA PDN

Para ejemplificar cómo cada sistema de la PDN se alimentará de distintas bases de datos, se utilizan a continuación los sistemas de información que resguarda la SFP, los cuales serán parte fundamental de la información a la que tendrá acceso el SNA a través de la Plataforma. Así mismo se presenta una tabla en que se clarifica cuáles conjuntos de información de la SFP alimentarán a cada sistema de la PDN.


BASES DE DATOS
RENIRESP
DECLARANET
RSPS SPAR
SIRA
SISTEMA 1
SISTEMA 2
SISTEMA 3
SISTEMA 4
SISTEMA 5
SISTEMA 6
COMPRANET
BEOP
SNA-SNF
SIDEC
SIINC-SACH
BASES DE DATOS

CLAVE	DENOMINACIÓN NORMATIVA	SISTEMAS DE LA SFP	ABREVIACIONES
S1	Sistema de evaluación patrimonial de declaración de intereses y constancia de presentación de declaración fiscal.	Sistema de Evolución Patrimonial de Declaración de Intereses y Constancia de Prestación de Declaración Fiscal	DECLARANET
S2	Sistema de los servidores públicos que intervengan en procedimientos de contrataciones públicas.	Registro de Servidores Públicos de la Administración Pública Federal que intervienen en procedimientos de contrataciones públicas	RENIRESP
S3	Sistema Nacional de servidores públicos y particulares sancionados.	Registro de Servidores Públicos Sancionados; Sistema de procedimientos administrativos de responsabilidades; Sistema Integral de Responsabilidades Administrativas	RSPS; SPAR; SIRA
S4	Sistema de información y comunicación del Sistema Nacional Anticorrupción y del Sistema Nacional de Fiscalización.	-	-
S5	Sistema de denuncias públicas de faltas administrativas y hechos de corrupción	Sistema Integral de Quejas y Denuncias Ciudadanas; Sistema integral de inconformidades; Sistema de procedimiento administrativo de sanción a proveedores y contratistas	SIDEC; SIINC; SACN
S6	Sistema de Información Pública de Contrataciones.	COMPRANET: Bitácora Electrónica de Obra Pública	COMPRANET; BEOP

" *(Sic)*.

Ahora bien, en relación con lo anterior es posible advertir que la PDN es un punto de conexión central en la cual interoperarán múltiples sistemas con cada uno de los seis sistemas de información que conforman la PDN, esto es que, gracias a la estandarización de la información, así como el uso de tecnología por medio de APIs, se realiza la interconexión entre diferentes fuentes de origen a saber:

- Con un ecosistema federal que incluya el conjunto de datos que generarán las entidades públicas a nivel federal, es decir, los Poderes Ejecutivo, Legislativo y Judicial, por los Órganos Constitucionalmente Autónomos, así como por las Empresas Productivas del Estado, y por cualquier otra entidad con naturaleza diferente a éstas que opere a nivel federal.
- Simultáneamente cada uno de los sistemas de la PDN deberá conectarse con los conjuntos de datos que hay en cada una de las 32 Entidades Federativas. Se deberá contemplar que cada Sistema Local Anticorrupción deberá contar con ese espejo de la PDN que contenga la

información que se genera en cada Entidad Federativa, y que, a través de cada Secretaria Ejecutiva de los Sistemas Locales, se concentrará y conectará la información con la PDN.

Asimismo, es importante precisar que, si bien, los sistemas de información que resguarda la Secretaría de Función Pública (tal como DeclaraNet, RENIRESP o el CompraNet, entre otros) serán parte fundamental de la información a la que tendrá acceso el SNA a través de la Plataforma y que proveerá a cada sistema de la misma, estas son sólo algunas de las bases de datos que conectarán con la PDN, pues el acceso y la interoperabilidad que se llevará a cabo a través de la PDN podrá realizarse con múltiples bases de datos de diferentes entes públicos a nivel federal y local.

Por lo tanto, a través de la PDN se realizará este cruce de múltiples sistemas de información a través de la interoperabilidad y las especificaciones técnicas que cada proveedor de estos sistemas debe de cumplir. Con ello se permitirá que en un solo espacio se realicen una interconexión de sistemas tanto de un ecosistema federal como local, aunado a que esta interconexión permitirá un acceso intenso a estos sistemas que, anteriormente no se llevaba a cabo.

Ahora bien, en el caso que nos ocupa, la SESNA manifestó que la implementación de la plataforma en comento contempla realizar un tratamiento frecuente y continúo de grandes volúmenes de datos personales, posterior al mes de mayo del presente año fecha límite en la que todos los servidores públicos de los tres órdenes de gobierno deben presentar sus declaraciones de situación patrimonial y de intereses en los formatos aprobados para tal efecto por el Comité Coordinador.

En este sentido, también se indicó que, por lo que refiere al S1, una vez que todos los sujetos obligados desarrollen las herramientas informáticas para conectarse a la PDN, se podrá consultar la información de 6 millones de personas servidoras públicas de todos los niveles de gobierno y órganos autónomos. Por lo que respecta a los sistemas S2 y S6, se indicó que el volumen de titulares de datos personales irá incrementando paulatinamente ya que depende de los procedimientos de contrataciones públicas, que se realicen, actualmente existen 346,453 registros.

En el S3, el volumen de titulares irá incrementando ya que depende de la resolución de los procedimientos sancionadores, más no se indica el total de registros que se tiene actualmente.

Derivado de lo anterior, este Instituto determina, con fundamento en los artículos 76 de la Ley General y 9, fracción VI, de las Disposiciones administrativas, que la puesta en operación de la PDN respecto de la interoperación e interconexión en dicho aplicativo actualiza un tratamiento intensivo o relevante de datos personales, ya que se realizarán cruces de información entre diversos sistemas que permitirá a los usuarios finales de la plataforma, realizar consultas de los sistemas fuentes y demás funcionalidades de acuerdo con cada perfil, mediante la conexión de datos desde los sistemas fuente

u origen hacia la plataforma. De igual forma, se llevará a cabo un tratamiento frecuente y continuo de grandes volúmenes de datos personales, conforme a lo informado por la SESNA.

VI. Identificación, análisis y gestión de los riesgos para la protección de los datos personales

Al respecto, La Ley General menciona que:

> *"**Artículo 33.** Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*
> *[...]*
> *III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;*
> *IV. Realizar un análisis de riesgo de los 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;*
> *V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*
> *VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*
> *[...]" (Sic).*

De conformidad con lo dispuesto en el artículo 33 fracciones III y IV de la Ley General, para establecer y mantener las medidas de seguridad para la protección de los datos personales el responsable debe elaborar un inventario de datos personales y de los sistemas de tratamiento, así como, realizar un análisis de riesgo de los 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; así como otras actividades interrelacionadas.

Adicionalmente, los Lineamientos Generales señalan que:

> ***"Análisis de riesgos***
>
> ***Artículo 60.** Para dar cumplimiento al artículo 33, fracción IV de la Ley General, el responsable deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:*
>
> *I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;*
> *II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;*
> *III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;*
> *IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y*

V. Los factores previstos en el artículo 32 de la Ley General.

Análisis de brecha

Artículo 61. *Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de brecha el responsable deberá considerar lo siguiente:*

I. Las medidas de seguridad existentes y efectivas;

II. Las medidas de seguridad faltantes, y

III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Plan de trabajo

Artículo 62. *De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.*

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes." (Sic).

Por su parte, el artículo 19 de las Disposiciones administrativas señala que:

*"**Artículo 19.** En la evaluación de impacto en la protección de datos personales, el responsable deberá incluir la gestión de riesgos que tenga por objeto identificar y analizar los posibles riesgos y amenazas, así como los daños o consecuencias que pudieran producirse o presentarse si llegasen a materializarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.*

El responsable deberá presentar un plan general para gestionar los riesgos identificados, en el que se mencione, al menos, lo siguiente:

I. La identificación y descripción específica de los riesgos administrativos, físicos o tecnológicos que podrían presentarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales;
II. La ponderación cuantitativa y/o cualitativa de la probabilidad de que los riesgos identificados sucedan, así como su nivel de impacto en los titulares en lo que respecta al tratamiento de sus datos personales, y
III. Las medidas y controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos detectados, de tal manera que no tengan un impacto en la esfera de los titulares, en lo que respecta al tratamiento de sus datos personales." (Sic).

De las disposiciones anteriores se advierte que el responsable está obligado a realizar un análisis de riesgo de los datos personales y los recursos involucrados en su tratamiento, considerando: (I) los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico; (II) el valor de los datos personales de acuerdo con la clasificación previamente definida y su ciclo de vida;

(III) el valor y exposición de los activos involucrados en el tratamiento de los datos personales; (IV) las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y (V) los factores previstos en el artículo 32 de la Ley General.

En particular, el responsable debe incluir la gestión de riesgos para identificar y analizar vulnerabilidades, amenazas, daños o consecuencias que pudieran materializarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.

Al respecto la SESNA manifestó lo siguiente:

> *"VI. IDENTIFICACIÓN, ANÁLISIS Y DESCRIPCIÓN DE LA GESTIÓN DE LOS RIESGOS INHERENTES*
>
> *Siguiendo la metodología de análisis de riesgo BAA21[16], se analizará el riesgo latente de los datos contenidos en cada sistema.*
>
> *• S1*
>
> *De acuerdo con la clasificación de riesgo inherente de la información propuesta en la metodología BAA, se concluye que, a través del S1, se podrán consultar datos de riesgo inherente bajo, medio y alto, ya que no sólo se tendrán datos de identificación de la persona servidora pública, su pareja y dependientes económicos, sino también datos relacionados con su patrimonio. Además, la información presentada en la declaración de intereses podría ser usada para inferir creencias religiosas, filosóficas, morales, afiliación sindical u opiniones políticas. Dada la combinación de datos personales que se podrían consultar a través de la PDN se concluye que el riesgo inherente debe ser clasificado como reforzado.*
>
> *También es necesario identificar el número de titulares de los que se tratarán datos personales. Se estima que, una vez que todos los sujetos obligados establezcan los protocolos de comunicación para conectarse a la PDN, se podrá consultar la información de 6 millones de personas servidoras públicas de todos los niveles de gobierno y órganos autónomos.*
>
> *Una vez definidos estos valores se puede determinar el nivel de riesgo por tipo de dato dentro del sistema. Es importante aclarar que, el sistema únicamente podrá distinguir entre la información que el Comité Coordinador clasificó como pública y reservada. Esto significa que cuando una persona, ya sea ciudadano o autoridad, consulte la información podrá ver, dependiendo de sus facultades, un conjunto de datos -de identificación, patrimoniales y de intereses-. Por esta situación se decidió hacer*

[16] El INAI desarrolló la Metodología BAA. Aunque no forma parte integral del documento de Recomendaciones en materia de Seguridad de los Datos Personales, el Instituto la presentó como una propuesta alternativa para cumplir con el deber de seguridad establecido en la LFPDPPP. Los tres factores que dan nombre a esta metodología son Beneficio, Accesibilidad y Anonimidad.

una valoración del conjunto de los datos -y no de forma individualizada- para determinar el nivel de riesgo.

Dados los diferentes tipos de datos que se podrán consultar en el sistema y el volumen de los titulares, se concluye que el nivel de riesgo es 5. Este es el nivel más alto para el factor Beneficio dentro de la metodología BAA.

La PDN opera con una arquitectura basada en comunicaciones a través de Internet, que permite consultar información desde diversos proveedores de información (Entes públicos), en tiempo real y de manera estandarizada (en un mismo formato). Esto significa que el único medio de consulta es por vía electrónica y no existen registros físicos, en posesión de la SESNA, respecto de la información consultable en la PDN.

Uno de los objetivos de la PDN es la rendición de cuentas y generar inteligencia por lo que garantizar el mayor grado de accesibilidad se considera como un elemento positivo. Sin embargo, se implementarán todas las medidas de seguridad necesarias para salvaguardar la secrecía de la información clasificada por el Comité Coordinador como confidencial y asegurar que únicamente las autoridades con facultades legales puedan acceder a estos datos.

Como ya se aclaró, el acceso será únicamente por Internet por lo que el nivel de anonimidad es 5, el más alto dentro de la metodología.

Factores	Valor
Beneficio	5
Accesibilidad	5
Anonimidad	5

En conclusión, la información que se podrá consultar a través del S1 es de alto riesgo. Sin embargo, es importante aclarar que la información no está almacenada en la PDN. Esta únicamente es un portal de acceso. Y segundo, existe un número importante de datos -la referente a la persona servidora pública- que, por acuerdo del Comité Coordinador del cual forma parte el INAI, será pública y otro conjunto de datos personales -de terceros- será clasificada y únicamente podrán tener acceso las autoridades competentes de acuerdo con la LGSNA y los procedimientos que apruebe el Comité Coordinador. Esto significa que la información que el Comité Coordinador calificó como pública debe estar disponible para toda la ciudadanía; por lo que las medidas de seguridad se concentrarán, principalmente, en salvaguardar la confidencialidad de la información clasificada como reservada.

• *S2*

A través de este sistema se podrán consultar datos de riesgo inherente bajo ya que únicamente contiene datos de identificación de las personas servidoras públicas que intervienen en procedimientos de contrataciones públicas. El volumen de titulares irá incrementando ya que depende de los procedimientos de contrataciones públicas que se realicen, los cuales forman parte de las funciones primordiales del Estado. Al unir estos dos valores podemos concluir que el nivel de riesgo es 1, el más bajo en la metodología.

Como se mencionó en el análisis del S1, el único medio de consulta es por internet y permite el acceso de un gran número de usuarios al mismo tiempo.

Factores	*Valor*
Beneficio	*1*
Accesibilidad	*5*
Anonimidad	*5*

- *S3*

Los datos consultables en este sistema son de riesgo inherente bajo ya que únicamente contiene datos de identificación de las personas servidoras públicas sancionadas. El volumen de titulares irá incrementando ya que depende de la resolución de los procedimientos sancionadores. Al unir estos dos valores podemos concluir que el nivel de riesgo es 1, el más bajo en la metodología.

Se reitera que el objetivo de la PDN es garantizar a toda la ciudadanía el acceso a la información pública por lo que se puede acceder al S3 por vía remota a través de internet.

Factores	*Valor*
Beneficio	*1*
Accesibilidad	*5*
Anonimidad	*5*

- *S6*

Los datos consultables en este sistema son de riesgo inherente bajo ya que únicamente contiene datos de identificación de las personas que intervienen en las contrataciones públicas, como servidoras públicas o como proveedores. El volumen de titulares irá incrementando ya que depende de las contrataciones públicas que se realicen, actualmente existen 346,453 registros. Al unir estos dos valores podemos concluir que el nivel de riesgo es 1, el más bajo en la metodología.

Los valores de accesibilidad y anonimidad son los mismos que para todos los sistemas de la PDN.

Factores	*Valor*
Beneficio	*1*
Accesibilidad	*5*
Anonimidad	*5*

Una vez definido el riesgo latente de los datos contenidos en cada sistema, se procederá al análisis de las vulnerabilidades de la Plataforma.

[...]

Vulnerabilidades

Es fundamental destacar que la PDN es una plataforma de interoperabilidad y, como lo establece la normatividad vigente (Bases de la PDN, LGRA, LGSNA), los Encargados son los responsables de recabar, ordenar y/o resguardar los datos e información en los subsistemas para su conexión con los sistemas de la PDN.

*1. **Incumplimiento de los Protocolos y normas de seguridad:** Es responsabilidad de los Encargados cumplir con todos los protocolos de seguridad emitidos y recomendados por la USTPDN para el tratamiento y transferencia de los datos. En caso de no cumplir con los protocolos y de darse*

una vulnerabilidad en términos de los datos y/o en el proceso de su transmisión, los Encargados deberán responder y realizar los ajustes necesarios para garantizar la seguridad de la información.

*2. **Mal uso de los datos:** sucede cuando un usuario – ciudadano o servidor público con facultades para acceder a información clasificada- transgrade los términos y condiciones de la PDN o las obligaciones contenidas en la LGPDPPSO.*

*3. **Información inexacta y/o equivocada**: Cuando los Encargados transfieren a la PDN información inexacta, campos adicionales, datos reservados y otro tipo de información que por sus características no debe ser pública o parte de la PDN.*

*4. **Acceso no autorizado:** Cuando se identifique o reporte un acceso a la PDN que caiga en alguno(s) de los siguientes supuestos: acceso sin autorización, contra derecho, habiendo obtenido de manera ilegal claves de acceso a un sistema con información reservada.*

*5. **Robo de dispositivos de infraestructura**: Dispositivos de almacenamiento o equipo de cómputo en los que se encuentre información sensible sobre la arquitectura o desarrollo de la PDN, configuraciones y otros datos que pudieran ser utilizados para acceder, transgredir o modificar la PDN y su contenido.*

Protocolo de actuación

*1. **Incumplimiento de los Protocolos y normas de seguridad:** la USTPDN ejecutará las siguientes acciones:*

• Las cuentas de usuario comprometidas con el acceso no autorizado, serán bloqueadas de inmediato por los administradores de la PDN.

• El incidente se notifica a los responsables del sistema, se documenta y se agrega a la bitácora en donde se registran todos los pasos hasta su remediación.

• Se extrae evidencia privilegiando su integridad.

• Se ejecutarán acciones concretas para intentar reparar, mitigar o contener los daños causados por el acceso no autorizado.

• En caso de no poder ser solventado por los administredores de la PDN, se revisará a un mayor nivel jerárquico para tomar las medidas pertinentes.

*2. **Mal uso de los datos**: Se identificará a los posibles responsables, en su caso, se eliminarán y bloquearán las cuentas y se notificará a los responsables de la información para que se realice una investigación y posible sanción.*

*3. **Información inexacta y/o equivocada:** Los Encargados deberán en todo momento revisar y asegurarse de que los datos interoperables con la PDN corresponden exclusivamente con la legislación vigente para cada uno de sus sistemas.*

En caso de que los datos personales contenidos en los expedientes sean inexactos o requieran actualizarse, se deberá realizar el procedimiento correspondiente con el Encargado, es decir la autoridad, ente o institución encargada de obtener y registrar la información en las bases de datos. Como lo establecen las Bases para el funcionamiento de la PDN, la información, su actualización y publicación es exclusivamente responsabilidad de los Encargados.

*4. **Acceso no autorizado**: Es fundamental mencionar que el acceso a los datos reservados se realizará con base en los permisos que el Comité Coordinador del SNA y con base en las atribuciones que la legislación aplicable confiere a aquellos que pueden consultar los datos reservados. En caso de que se registre un acceso no autorizado, se debe identificar de dónde provino y cómo fue el acceso.*

***A través de usuario registrado y con privilegios**. Al generar un acceso mediante usuario y contraseña a la PDN que tenga privilegios para la consulta de información confidencial, se le confiere la completa responsabilidad al usuario, del buen uso, resguardo y confidencialidad de sus datos de usuario y contraseña. En caso de existir el robo o uso ilegal de su usuario y contraseña, el usuario debe notificar inmediatamente al personal de la SESNA para bloquear esa cuenta. Se hará un rastreo de los datos que se consultaron, la fecha y la hora. Se notificará al usuario sobre la información que se consultó.*

***Resguardo de usuarios y contraseñas para acceder a datos reservados**:. Las credenciales, listas de permisos y contraseñas se resguardarán en una Base de Datos segura que podrá ser consultada únicamente por los Encargados y el equipo administrador de la PDN. La Base de Datos segura contará con el soporte de las cuatro capas de seguridad antes mencionadas (**Sistema Operativo, Aplicaciones, Segmento de red y Red perimetral**). Asimismo, en la Base de Datos las contraseñas de acceso se encontrarán cifradas para evitar que puedan ser visibles a ojo humano o utilizadas para acceder al sistema en el supuesto caso de que un atacante llegara a sustraerlas de la PDN.*

*5. **Robo de dispositivos de infraestructura**: Se deberá notificar inmediatamente al superior jerárquico y al equipo de la USTPDN sobre el robo o desaparición de los dispositivos o infraestructura aplicable. Se hará un análisis sobre los datos que contenían y se realizarán las medidas necesarias para la contención o mal manejo de cualquier información.*

VII. CICLO DE VIDA DE LOS DATOS PERSONALES

La PDN no recaba, almacena, ni genera los datos consultables en cada sistema. Por lo tanto, no tiene acceso a las bases de datos ni tiene facultades para capturar, modificar o eliminar los datos contenidos en cada sistema. A través de la Plataforma se podrán consultar datos contenidos en diversas bases de datos, en tiempo real y de forma estandarizada.

Los plazos de conservación o almacenamiento de los datos personales y las técnicas para el borrado seguro de los datos será responsabilidad de las instituciones, dependencias u organismos que recaban la información y dueños de las bases de datos.

[...]" (Sic).

Adicionalmente en el Anexo a la evaluación de impacto en la protección de datos personales presentada por la SESNA a efectos de ser consultado como información adicional para la misma, se indicó lo siguiente:

"***• ANÁLISIS DE RIESGOS.***

Siguiendo la metodología de análisis de riesgo BAA3, se analizará el riesgo latente de los datos contenidos en cada sistema.

• S1

De acuerdo con la clasificación de riesgo inherente de la información propuesta en esta metodología, se concluye que, a través del S1, se podrán consultar datos de riesgo inherente bajo, medio y alto ya que no sólo se tendrán datos de identificación de la persona servidora pública, su pareja y dependientes económicos, sino también datos relacionados con su patrimonio. Además, con la información presentada en la declaración de intereses se podría inferir creencias religiosas, filosóficas, morales, afiliación sindical u opiniones políticas. Dada la combinación de datos personales que se podrían consultar a través de la PDN se concluye que el riesgo inherente debe ser clasificado como reforzado.

También es necesario identificar el número de titulares de los que se tratarán datos personales. Se estima que, una vez que todos los sujetos obligados desarrollen las herramientas informáticas para conectarse a la PDN, se podrá consultar la información de 6 millones de personas servidoras públicas de todos los niveles de gobierno y órganos autónomos.

Una vez definidos estos valores se puede determinar el nivel de riesgo por tipo de dato dentro del sistema. Es importante aclarar que, el sistema únicamente podrá distinguir entre la información que el Comité Coordinador clasificó como pública y reservada. Esto significa que cuando una persona, ya sea ciudadano o autoridad, consulte la información podrá ver un conjunto de datos -de identificación, patrimoniales y de intereses-. Por esta situación se decidió hacer una valoración del conjunto de los datos para determinar el nivel de riesgo.

Dado los diferentes tipos de datos que se podrán consultar en el sistema y al volumen de los datos, se concluye que el nivel de riesgo es 5. Este es el nivel más alto para el factor Beneficio dentro de la metodología BAA.

La PDN opera con una arquitectura basada en comunicaciones a través de Internet, que permite consultar información desde diversos proveedores de información (Entes públicos), en tiempo real y de manera estandarizada (en un mismo formato). Esto significa que el único medio de consulta es por vía electrónica y no existen registros físicos, en posesión de la SESNA, respecto de la información consultable en la Plataforma.

Uno de los objetivos de la PDN es la rendición de cuentas y generar inteligencia artificial por lo que garantizar el mayor grado de accesibilidad se considera como un elemento positivo. Sin embargo, se implementarán todas las medidas de seguridad necesarias para salvaguardar la secrecía de la información clasificada como confidencial y asegurar que únicamente las autoridades con facultades legales puedan acceder a estos datos.

Como ya se aclaró, el acceso será únicamente por Internet por lo que el nivel de anonimidad es 5, el más alto dentro de la metodología.

Factores	Valor
Beneficio	5
Accesibilidad	5

Anonimidad	5

En conclusión, la información que se podrá consultar a través del S1 es de alto riesgo. Sin embargo, es importante aclarar, antes de señalar las medidas de seguridad que se implementarán, que la información no está almacenada en la PDN. Esta únicamente es un portal de acceso. Y segundo, existe un número importante de datos -la referente a la persona servidora pública- que será pública y otro conjunto de datos personales -de terceros- que será clasificada y únicamente podrán tener acceso las autoridades competentes de acuerdo con la LGSNA y los procedimientos que emita el Comité Coordinador. Esto significa que la información que el Comité Coordinador calificó como pública debe estar disponible para toda la ciudadanía; por lo que las medidas de seguridad se concentrarán, principalmente, en salvaguardar la confidencialidad de la información clasificada como reservada.

• S2

A través de este sistema se podrán consultar datos de riesgo inherente bajo ya que únicamente contiene datos de identificación de las personas servidoras públicas que intervienen en procedimientos de contrataciones públicas. El volumen de titulares irá incrementando ya que depende de los procedimientos de contrataciones públicas que se realicen, los cuales forman parte de las funciones primordiales del Estado. Al unir estos dos valores podemos concluir que el nivel de riesgo es 1, el más bajo en la metodología.

Como se mencionó en el análisis del S1, la PDN opera con una arquitectura basada en comunicaciones a través de Internet, que permite consultar información desde diversos proveedores de información (Entes públicos), en tiempo real y de manera estandarizada (en un mismo formato). Esto significa que el único medio de consulta es por internet y permite el acceso de un gran número de usuarios al mismo tiempo.

Factores	Valor
Beneficio	1
Accesibilidad	5
Anonimidad	5

• S3

Los datos consultables en este sistema son de riesgo inherente bajo ya que únicamente contiene datos de identificación de las personas servidoras públicas sancionadas. El volumen de titulares irá incrementando ya que depende de la resolución de los procedimientos sancionadores. Al unir estos dos valores podemos concluir que el nivel de riesgo es 1, el más bajo en la metodología.

Se reitera que el objetivo de la PDN es garantizar a toda la ciudadanía el acceso a la información pública por lo que se puede acceder al S3 por vía remota a través de internet.

Factores	Valor
Beneficio	1
Accesibilidad	5
Anonimidad	5

• S6

Los datos consultables en este sistema son de riesgo inherente bajo ya que únicamente contiene datos personales de identificación de las personas que intervienen en las contrataciones públicas, como servidoras públicas o como proveedores. El volumen de titulares irá incrementando ya que depende de las contrataciones públicas que se realicen, actualmente existen 346 453 registros. Al unir estos dos valores podemos concluir que el nivel de riesgo es 1, el más bajo en la metodología.

Se reitera que el objetivo de la PDN es garantizar a toda la ciudadanía el acceso a la información pública por lo que se puede acceder al S6 por vía remota a través de internet.

Factores	Valor
Beneficio	1
Accesibilidad	5
Anonimidad	5

Es importante aclarar que todas las consultas a la información contenida en los sistemas de tratamiento de datos personales de la PDN se realizan a través de servicios web o API's por lo que no existen soportes físicos que deban ser resguardados.

*Los **mecanismos de seguridad** que se ejecutan para el debido manejo del sistema de tratamiento de datos personales son los siguientes:*

1. Transferencias y Remisiones. - Se realizan de conformidad con lo siguiente:

a) *De traslado sobre redes electrónicas: La SESNA utiliza una red privada virtual bajo el protocolo IPSec para establecer un canal seguro de comunicación entre los Encargados y la PDN.*
b) *El Encargado y la SESNA cuentan con sistemas y/o protocolos de detección de intrusos (IDS) para asegurar que las transferencias se llevan a cabo únicamente entre el Encargado y la PDN, identificando cualquier actividad o flujo de información atípicos. Las transmisiones se registran en una bitácora electrónica que se controla de manera interna.*
c) *La selección de la información que se transfiere entre Encargados y la SESNA se da con base en las consultas realizadas por los usuarios de la PDN. Por ende, las transferencias de información de las bases de datos del Encargado a la PDN únicamente se dan como resultado de una consulta.*
d) *La consulta de información a través de la PDN puede hacerse anónimamente siempre se trate de información no reservada.*
e) *Al generar una consulta pública en la PDN, únicamente se transfiere la información no reservada de los Encargados. En ese sentido, los Encargados deberán evitar exponer registros completos, con información adicional a la que se puede obtener de manera pública y anónima.*
f) *La consulta de información reservada en ningún caso se puede realizar de manera anónima y se requiere de permisos especiales para que el Encargado y la PDN faciliten el acceso a ella a usuarios bien identificados.*

2. Bitácoras para accesos y operación cotidiana.

a) *La PDN permite la consulta de información no reservada de manera pública y anónima, por lo cual, se cuenta con un registro con fines estadísticos que permite identificar búsquedas frecuentes y otras métricas de uso.*

b) Para el acceso a la información reservada, será necesario iniciar sesión en la PDN a través de un usuario y contraseña. También, en una segunda etapa se contará con la opción de inicio de sesión a través de la firma electrónica.
c) El acceso a la información reservada se encuentra restringido a los servidores públicos que tengan las facultades y atribuciones legales para poder consultar esta información reservada. Todo acceso a información reservada deberá ser registrado por el Encargado y la PDN.
d) Los Encargados y la SESNA contarán con una base de datos que incluirá la información necesaria para identificar a los servidores públicos y sus respectivas facultades para acceso a la información reservada.
e) El registro del acceso a la información reservada deberá contener al menos los siguientes datos:
   i. Usuario que realizó la consulta
   ii. Nombre del servidor público
   iii. Datos de adscripción del servidor público (Institución, unidad, etc.)
   iv. Parámetros de consulta (el objeto de la búsqueda)
   v. Fecha de la consulta

3. Registro de incidentes. - En caso de suceder algún incidente que implique la divulgación de información reservada o el mal uso de los datos personales consultables en la PDN:

a) El incidente se documenta y se agrega a la bitácora en donde se registra cualquier tipo de incidente de esta índole.
b)
c) Se dará aviso al Encargado de la generación e interoperabilidad de los datos acerca del incidente en cuestión para tomar las medidas correctivas adecuadas.

4. Los Encargados y la PDN realizarán periódicamente verificaciones a sus sistemas informáticos para reducir el riesgo de brechas de información. Se deberán al menos realizar las siguientes verificaciones:

a) Parcheo y actualización de software.
b) Cifrado fuerte de datos para datos sensibles.
c) Mejora, renovación y actualización de dispositivos (por ejemplo, equipos que ya no cuentan con soporte por parte del proveedor).
d) Reforzar políticas de uso de dispositivos personales (por ejemplo, requerir que sa use un servicio de Red Privada Virtual o VPN y software antivirus).
e) Uso de contraseñas fuertes y autenticación multi factor.
f) Capacitación del personal en mejores prácticas de seguridad informática y estrategias para reducir riesgos por ataques de ingeniería social.

2. Doble factor de autenticación, mediante un código obtenido por una aplicación, correo electrónico y/o mensaje SMS que valide la identidad del usuario de la PDN.

3. Los sistemas en donde se aloja la PDN cuentan con al menos cuatro capas de defensa las cuales se mencionan a continuación: Sistema Operativo, Aplicaciones, Segmento de red y red perimetral.

4. *Política de contraseñas seguras mediante el uso de contraseñas largas, con combinaciones complejas de caracteres que incluyan mayúsculas, minúsculas, números y signos de puntuación o símbolos, considerando sean cambiadas cada 90 días.*

5. *Los responsables deberán atender siempre las recomendaciones emitidas por la USTPDN respecto a los protocolos, niveles y medidas de seguridad para lograr la interoperabilidad con la PDN. De no atenderse, la USTPDN se reserva el derecho a realizar la conexión de sus sistemas con la PDN.*

Riesgos detectados

Es fundamental destacar que la PDN es una plataforma de interoperabilidad, y como lo establece la normatividad vigente (Bases de la PDN, LGRA, LGSNA), los Encargados son los responsables de recibir, ordenar y/o resguardar los datos e información en los subsistemas para su integración a los sistemas de la PDN.

- ***Incumplimiento de los Protocolos y normas de seguridad:*** *Es responsabilidad de los Encargados cumplir con todos los protocolos de seguridad emitidos y recomendados por la USTPDN para el tratamiento y transferencia de los datos. En caso de no cumplir con los protocolos y de darse una vulnerabilidad en términos de los datos y/o en el proceso de su transmisión, los Encargados deberán responder y realizar los ajustes necesarios para garantizar la seguridad de la información.*
- ***Mal uso de los datos:*** *sucede cuando un servidor público con facultades para acceder a información pública o clasificada transgrede los términos y condiciones de la PDN o las obligaciones contenidas en la LGPDPPSO.*
- ***Información inexacta y/o equivocada:*** *Cuando los Encargados transfieren a la PDN información inexacta, campos adicionales, datos reservados y otro tipo de información que por sus características no debe ser pública o parte de la PDN.*
- ***Acceso no autorizado:*** *En el caso en el que se identifique o reporte un acceso a la PDN que caiga en alguno(s) de los siguientes supuestos: acceso sin autorización, contra derecho, habiendo obtenido de manera ilegal claves de acceso a un sistema con información reservada.*

Robo de dispositivos de infraestructura: *Dispositivos de almacenamiento o equipo de cómputo en los que se encuentre información sensible sobre la arquitectura o desarrollo de la PDN, configuraciones y otros datos que pudieran ser utilizados para acceder, transgredir o modificar la PDN y su contenido.*

Protocolo de actuación:

- Incumplimiento de los Protocolos y normas de seguridad: *la USTPDN ejecutará las siguientes acciones:*

- *Las cuentas de usuario comprometidas con el acceso no autorizado, serán bloqueadas de inmediato por los administradores de la PDN.*
- *El incidente se notifica a los responsables del sistema, se documenta y se agrega a la bitácora en donde se registran todos los pasos hasta su remediación.*
- *Se extrae evidencia privilegiando su integridad.*
- *Se ejecutarán acciones concretas para intentar reparar, mitigar o contener los daños causados por el acceso no autorizado.*

- *En caso de no poder ser solventado por los administradores de la PDN, se revisará a un mayor nivel jerárquico para tomar las medidas pertinentes.*

-Mal uso de los datos: *Se identificará a los posibles responsables, en su caso, se eliminarán y bloquearán las cuentas y se notificará a los responsables de la información para que se realice una investigación y posible sanción.*

-Información inexacta y/o equivocada: *Los Encargados deberán en todo momento revisar y asegurarse de que los datos interoperables con la PDN corresponden exclusivamente con la legislación vigente para cada uno de sus sistemas.*
Acceso no autorizado

En caso de que los datos personales contenidos en los expedientes sean inexactos o requieran actualizarse, se deberá realizar el procedimiento correspondiente con el Encargado, es decir la autoridad, ente o institución encargada de obtener y registrar la información en las bases de datos. Como lo establecen las Bases para el funcionamiento de la PDN, la información, su actualización y publicación es exclusivamente responsabilidad de los Encargados.

-Acceso no autorizado

-Robo de dispositivos de infraestructura: *Se deberá notificar inmediatamente al superior jerárquico y al equipo de la USTIPDN sobre el robo o desaparición de los dispositivos o infraestructura aplicable. Se hará un análisis sobre los datos que contenían y se realizarán las medidas necesarias para la contención o mal manejo de cualquier información.*

6. ANÁLISIS DE BRECHA.

- *Los Encargados deberán de resguardar en todo momento los datos personales mediante sistemas de archivos o bases de datos cifradas antes de su envío o interoperabilidad con la PDN.*
- *Los Encargados y la SESNA deberán contar con sistemas o protocolos de detección de intrusos (IDS) para asegurar que las transferencias se llevan a cabo únicamente entre el Encargado y la PDN, identificando cualquier actividad o flujo de información atípicos.*
- *La comunicación entre los Encargados y la SESNA deberá llevarse a cabo mediante una Red Privada Virtual o VPN para todos los sistemas de la PDN.*
- *Los usuarios que tengan la facultad de consultar información de carácter reservado deberán de acceder con firma electrónica avanzada.*
- *Se considera que se tienen medidas de seguridad óptimas para el resguardo de la información personal por parte de la PDN. Sin embargo, dado que la información es incorporada a la PDN por los Encargados, es fundamental que estos últimos implementen las estrategias y políticas para prevenir y mitigar los riesgos expuestos en el presente documento.*

*7. **PLAN DE TRABAJO***

Unidad de Servicios Tecnológicos y Plataforma Digital Nacional
Plataforma Digital Nacional

Plan de trabajo 2021-2022		
Medidas de seguridad a implementar	**Responsable**	**Descripción**
Documentar y desarrollar análisis de vulnerabilidades para la PDN	USTPDN	Identificar y documentar los riesgos que puedan comprometer a los sistemas de la PDN mediante pruebas internas y externas a la infraestructura de la SESNA, elaborando un plan de remediación que permita reducir el riesgo de ataques informáticos.
Documentar y desarrollar el análisis de riesgos que los identifique, clasifique y priorice según su impacto, en los procesos y servicios contemplados en la PDN.	USTPDN	Elaboración de un análisis que permita identificar y clasificar cualquier tipo de riesgo y su impacto, en todos los procesos de uso y transferencia de datos de la PDN
Generar un proceso de fortalecimiento de la seguridad y mejora continua de controles.	USTPDN	Con las conclusiones y recomendaciones de los análisis de riesgos y vulnerabilidades, se implementarán medidas de mejora y fortalecimiento de los controles de la PDN.
Elaborar plan de respuesta ante incidente.	USTPDN	Desarrollar un protocolo de actuación que contemple las respuestas y acciones a tomar en caso de que se registre cualquier tipo de incidente.
Generar una Red Privada Virtual o VPN	USTPDN + Encargados	Robustecer los canales de comunicación seguros con cifrado en la transmisión de datos entre los Encargados y la SESNA para todos los sistemas de la PDN.

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

Como mecanismos de monitoreo, se utilizan las auditorías que registran los accesos a sistemas y datos de todos los usuarios con el objetivo de detectar posibles riesgos de seguridad.

Los registros de auditoría deberán incluir:

1. *Identificación del usuario.*
2. *Fecha de inicio y fin.*

3. *Registros de intentos exitosos y fallidos de acceso a los sistemas.*
4. *Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.*

En todos los casos, los registros de auditoria serán archivados preferentemente en un equipo diferente al que los genere, la periodicidad de las revisiones se realizará de manera semestral.

Monitoreo del Uso de los Sistemas

Se realiza un monitoreo sobre el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente. La periodicidad de las revisiones se realizará de manera semestral.

Todos el personal de la USTPDN debe conocer el alcance preciso del uso adecuado de los recursos informáticos, así como las actividades que pueden ser objeto de control y monitoreo.

Entre los eventos que deben tenerse en cuenta para el control y monitoreo de los sistemas, se enumeran las siguientes:

1. *Acceso no autorizado, incluyendo detalles como:*
   a) *Identificación del usuario.*
   b) *Fecha y hora de eventos clave.*
   c) *Tipos de eventos.*
   d) *Archivos a los que se accede.*

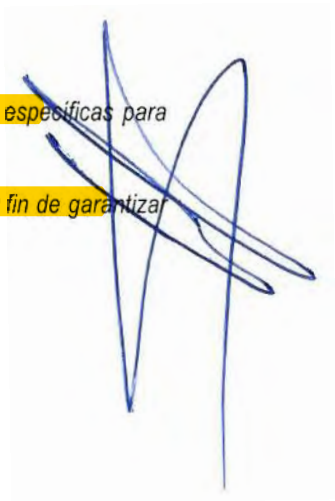
2. *Todas las operaciones con privilegio, como:*
   a) *Uso de cuenta de administrador.*
   b) *Inicio y cierre del sistema.*
   c) *Conexión y desconexión de dispositivos de ingreso y salida de información o que permitan copiar datos.*
   d) *Cambio de fecha/hora.*
   e) *Cambios en la configuración de la seguridad.*
   f) *Alta de servicios.*

3. *Intentos de acceso no autorizado, como*
   a) *Intentos fallidos.*
   b) *Violaciones de accesos y notificaciones para "Gateways" y "Firewalls".*
   c) *Alertas de sistemas de detección de intrusiones.*

4. *Alertas o fallas de sistema como:*
   a) *Alertas o mensajes de consola.*
   b) *Excepciones del sistema de registro.*
   c) *Alarmas del sistema de administración de redes.*

Registro y Revisión de Eventos

Registro y revisión de los eventos de auditoria, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados.



La periodicidad de dichas revisiones es de manera semestral, utilizando herramientas específicas para auditoría o utilitarios adecuados para llevar a cabo el control de los registros.

Las herramientas de registro deberán contar con los controles de acceso necesarios, a fin de garantizar que no ocurra:

1. *La desactivación de la herramienta de registro.*
2. *La alteración de mensajes registrados.*
3. *La edición o supresión de archivos de registro.*
4. *La saturación de un medio de soporte de archivos de registro.*
5. *La falla en los registros de los eventos.*
6. *La sobre escritura de los registros.*

9. PROGRAMA GENERAL DE CAPACITACIÓN

*La Unidad de Transparencia difundirá su programa de capacitación y actualización para los servidores públicos de la **SESNA** en materia de protección de datos personales al que está obligado a establecer el Comité de Transparencia de conformidad con lo dispuesto en el artículo 84 fracción VII de la **LGPDPPSO**, a efecto de que dichos servidores públicos se capaciten respecto de la protección de datos personales y ejercicio de derechos ARCO. También se desarrollará un programa de capacitación especializado para las personas servidoras públicas que sean responsables del tratamiento y protección de datos personales.*

Adicionalmente a los cursos impartidos por el INAI, se prevé la contratación de capacitadores externos para garantizar un mayor nivel de especialización en las prácticas y conocimiento de los servidores públicos responsables del tratamiento de los datos personales." (Sic)

En este sentido, para cumplir con la identificación, análisis y gestión de los riesgos para la protección de datos personales, la SESNA deberá atender lo dispuesto en los artículos 33 de la Ley general, 60, 61 y 62 de los Lineamientos generales y 19 de las Disposiciones administrativas.

Por lo tanto, para la Evaluación de Impacto que nos ocupa, se identifica que a partir de la información presentada tanto en su escrito inicial como en la correspondiente al Requerimiento de Información Adicional, no se visualizan los elementos establecidos en los artículos 33, de la Ley General y 60, de los Lineamientos Generales.

De igual forma, se debe indicar que el análisis de riesgos no sólo tendría que suscribirse al ámbito técnico, sino a los elementos que previene la Ley General sobre el particular, como son las medidas de seguridad administrativas y físicas, así como los supuestos establecidos en su artículo 32, y, los requerimientos normativos derivados, contemplando todos los elementos inherentes al funcionamiento de la plataforma y las operaciones que se realizarán en la misma toda vez que es ahí donde se encuentre l propio riesgos. De igual forma, es importante precisar que la SESNA no refiere políticas ni lineamientos internos para la gestión y tratamiento de los datos personales, ni se acredita la capacitación en materia de datos personales.

Por lo que este Instituto recomienda, realizar las siguientes acciones:

- Identificar adecuadamente el marco normativo y técnico aplicable al marco de actuación de la SESNA, y, en su caso, señalar expresamente las razones justificaciones por las cuales la gestión no hace uso de dichos instrumentos, como podría ser el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información, Comunicaciones y de Seguridad de la Información (MAAGTICSI).
- Fortalecer el análisis de riesgos a la PDN sobre los riesgos no sólo que respecto del ámbito técnico y deberá contemplar al menos lo siguiente:
  I. La identificación y descripción específica de los riesgos administrativos, físicos o tecnológicos;
  II. La ponderación cuantitativa y/o cualitativa de la probabilidad de que los riesgos identificados sucedan, así como su nivel de impacto en los titulares en lo que respecta al tratamiento de sus datos personales, y
  III. Las medidas y controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos detectados.

  Para tales efectos se sugiere identificar la técnica para el análisis de riesgos más conveniente conforme el marco de referencia adoptado; para lo cual, a su vez, habrá de considerarse lo establecido en el artículo 32 de la Ley General.
- Realizar un análisis de brecha, esto es, que el análisis se deberá realizar el comparativo entre las medidas de seguridad existentes y que son efectivas contra las medidas de seguridad que faltarían, cuyos resultados permitirían al responsable establecer las medidas de seguridad que podrían remplazar a uno o más controles implementados actualmente para la conexión entres sistemas de la PDN y sobre el funcionamiento de la misma.
- Elaborar un plan de trabajo para la implementación de los requerimientos normativos y las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales a través de la PDN así como de los sistemas fuentes de dónde se origina la información para consulta desde la plataforma, para lo cual se deberá tomar en cuenta los recursos destinados, el personal interno y externo de la SESNA y las fechas de compromiso para la implementación de dichas medidas nuevas o faltantes.

De las consideraciones anteriores, el Instituto determina oportunidades para fortalecer con la identificación, análisis y gestión de los riesgos para la protección de los datos personales a que hace referencia el artículo 19 de las Disposiciones administrativas.

VII. Mecanismos o procedimientos para que la puesta en operación de la PDN cumpla con las obligaciones previstas en la Ley General y demás disposiciones aplicables.

De conformidad con las manifestaciones y documentos presentados por la SESNA y en lo dispuesto en los artículos 74 y 77 de la Ley General y 10 y 11 de las Disposiciones administrativas, se procede a realizar el análisis de cumplimiento respecto de la puesta en operación de la PDN.

1. Principios

1.1. Principio de licitud

El artículo 17 de la Ley General dispone lo siguiente:

> "***Artículo 17.*** *El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera." (Sic).*

Por su parte, el artículo 8 de los Lineamientos generales establece que:

> "***Principio de licitud***
> ***Artículo 8.*** *En términos del artículo 17 de la Ley General, el responsable deberá tratar los datos personales que posea sujetándose a las atribuciones o facultades que la normatividad aplicable le confiera, así como con estricto apego y cumplimiento de lo dispuesto en dicho ordenamiento, los presentes Lineamientos generales, la legislación mexicana que le resulte aplicable y, en su caso, el derecho internacional, respetando los derechos y libertades de los titulares." (Sic).*

De lo anterior se desprende que todo tratamiento de datos personales debe sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera al responsable. Es por ello, que el responsable está obligado a identificar aquellas facultades o atribuciones, en la normatividad que le resulte aplicable, que lo habiliten para realizar cualquier tratamiento de datos personales.

Asimismo, el responsable está obligado a tratar los datos personales en su posesión con estricto apego y cumplimiento de la legislación mexicana y, en su caso, el derecho internacional que resulte aplicable a dicho tratamiento.

Sobre el particular, en la presentación de la evaluación de impacto que nos ocupa, la SESNA manifestó lo siguiente sobre el principio de licitud:

*"El artículo 9, fracción XIII de la Ley General del Sistema Nacional Anticorrupción (**LGSNA**) señala que el Comité Coordinador tiene la facultad de establecer "una Plataforma Digital Nacional que integre y conecte los diversos sistemas electrónicos que posean datos e información necesaria para que las autoridades competentes tengan acceso a los sistemas a que se refiere el Título Cuarto de esta Ley"5. Estos sistemas son, según lo dispone el artículo 49 de la LGSNA, al menos los siguientes:*

1. Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal. (S1)
2. Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas. (S2)
3. Sistema nacional de Servidores públicos y particulares sancionados. (S3)
4. Sistema de información y comunicación del Sistema Nacional y del Sistema Nacional de Fiscalización. (S4)
5. Sistema de denuncias públicas de faltas administrativas y hechos de corrupción. (S5)
6. Sistema de Información Pública de Contrataciones. (S6)

La LGSNA también señala en el párrafo segundo del artículo 48, que el Secretario Técnico, titular de la SESNA, será el encargado de administrar las plataformas digitales que establezca el Comité Coordinador del Sistema Nacional Anticorrupción (Comité Coordinador).

El Comité Coordinador, en cumplimiento de sus atribuciones, emitió las Bases para el funcionamiento de la PDN las cuales establecen las directrices para el funcionamiento de la PDN y los sistemas que la conforman, buscando garantizar la interoperabilidad, interconexión, estabilidad, uso y seguridad de la información integrada en la Plataforma Digital Nacional; promoviendo la homologación de procesos, estandarización de datos y la simplicidad del uso para los usuarios; teniendo en cuenta en todo momento los derechos de acceso a la información y protección de datos personales en posesión de los sujetos obligados.
[…]

Con el objetivo de incorporar datos a la PDN, los generadores de información deben establecer mecanismos tecnológicos que permitirán la consulta de información desde la PDN hacia sus bases de datos. En ese sentido, la SESNA publicó las Especificaciones Técnicas y Estándares de Datos que permiten que cualquier Ente público[9] pueda desarrollar y poner en marcha los mencionados mecanismos de comunicación.
*[9] Con fundamento en el artículo 3, fracción X de la Ley General de Responsabilidades Administrativas, **Ente Público** contempla:*
Los Poderes Legislativo y Judicial, los órganos constitucionales autónomos, las dependencias y entidades de la Administración Pública Federal, y sus homólogos de las entidades federativas, los municipios y alcaldías de la Ciudad de México y sus dependencias y entidades, la Procuraduría General de la República y las fiscalías o procuradurías locales, los órganos jurisdiccionales que no formen parte de los poderes judiciales, las Empresas productivas del Estado, así como cualquier otro ente sobre el que tenga control cualquiera de los poderes y órganos públicos citados de los tres órdenes de gobierno.
[…]

El fundamento para la construcción de la PDN lo encontramos en:
1. *Artículos 9, fracción XIII, 48, 49 de la Ley General del Sistema Nacional Anticorrupción;*
2. *Ley General de Responsabilidades Administrativas (artículos 26, 27,30, 31, 34, 43,44, 46, 59, 93)*

3. Las Bases para el funcionamiento de la PDN, publicadas en el Diario Oficial de la Federación el día 23 de octubre de 2018.
Se reitera que actualmente únicamente están en operación cuatro de los seis sistemas que integran la PDN, por lo que únicamente se presentará información respecto de esos sistemas.

[...]

INFORMACIÓN DEL SISTEMA S1

[...]

Además, se debe destacar que de acuerdo con el artículo 40 de las Bases de la PDN, el S1 estará conformado por los datos resguardados por los encargados, a través de sus sistemas de declaración patrimonial, de intereses e inscripción de constancia de la declaración anual de impuestos. Estos datos serán estandarizados de acuerdo con las especificaciones emitidas por la SESNA.

La Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos, según corresponda, se deben coordinar con la SESNA para establecer los mecanismos de integración y conexión de la información contenida en los sistemas electrónicos a través de los cuales los servidores públicos presenten las declaraciones. Lo anterior se contempla en el artículo 41 de las enunciadas Bases de la PDN.

Adicionalmente, la SESNA debe establecer los mecanismos para que la información del sistema sea solicitada y utilizada de acuerdo con las necesidades de las diversas autoridades competentes, entre las que se encuentran el Ministerio Público, Tribunal eso autoridades judiciales, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras, entre otras, en el ejercicio de sus respectivas atribuciones, previa aprobación del Comité Coordinador.

Por último, en términos de los artículos 42 a 45 de las Bases para la PDN, la SESNA establecerá un portal del sistema para dar acceso a la ***información pública*** *de las declaraciones de situación patrimonial y de intereses a todos los ciudadanos; un mecanismo que permita que la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos realicen la verificación aleatoria de las declaraciones patrimonial, de intereses, y para identificar la evolución del patrimonio de los servidores públicos, así como un mecanismo para la expedición de certificaciones de la inexistencia de anomalías, las cuales deberán anotarse en el sistema.*
[...]

INFORMACIÓN DEL SISTEMA S2

[...]

A su vez, el artículo 46 de las Bases para el funcionamiento de la PDN, establece que el objeto del S2 es permitir que los distintos usuarios tengan acceso a la información relacionada con los servidores públicos que intervienen en procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, de tal manera que sea utilizada por los integrantes del Sistema Nacional Anticorrupción y autoridades

competentes en sus funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.

Además de lo anterior, el artículo 47 de las enunciadas Bases establece que ***el S2 estará conformado por los datos resguardados por los Encargados,***[15] ***de acuerdo con los formatos especificados por el Comité Coordinador****. Estos datos deberán ser actualizados de manera quincenal por los entes e* ***incluirán, como mínimo, los nombres y adscripción de los servidores públicos que intervengan en contrataciones, así como la relación de particulares, personas físicas y morales que se encuentren inhabilitados para celebrar contratos con los entes públicos,*** *derivado de procedimientos administrativos diversos a los previstos en la Ley General de Responsabilidades Administrativas.*

Como información relevante se debe manifestar que, en el mes de febrero del 2019, se publicó en la página de la PDN el estándar de datos para lograr la interoperabilidad del S2 con la PDN.

El estándar de datos del S2 está disponible en: https://plataformadigitalnacional.org/intervienen/especificaciones

Los campos y el diccionario de datos que contiene este sistema se encuentran en: https://docs.google.com/spreadsheets/d/1fRhDfHtrBPYyR36zxpenXWind9FP1pLAQJOVS69QwUM/edit#gid=262781770
[...]" (Sic).

II. Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas;

3. Artículos 46, 47 y 48 de las Bases para el funcionamiento de la PDN.

"Artículo 46. *El objeto del sistema es permitir que los distintos usuarios tengan acceso a la información relacionada con los servidores públicos que intervienen en procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, de tal manera que sea utilizada por los integrantes del Sistema Nacional Anticorrupción y autoridades competentes en sus funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.*

Artículo 47. *El sistema estará conformado por los datos resguardados por los encargados, de acuerdo a los formatos especificados por el Comité Coordinador. Estos datos deberán ser actualizados de manera quincenal por los entes e incluirán, como mínimo, los nombres y adscripción de los servidores públicos que intervengan en contrataciones, así como la relación de particulares, personas físicas y morales que se encuentren inhabilitados para celebrar contratos con los entes públicos, derivado de procedimientos administrativos diversos a los previstos en la Ley de Responsabilidades.*

Artículo 48. *La Secretaría Ejecutiva establecerá un portal de internet, a través del cual se ponga a disposición de todo público los datos públicos a que se refiere el presente capítulo."*
[...]

INFORMACIÓN DEL SISTEMA S3

[...]

Asimismo, el artículo 50 de las Bases para el funcionamiento de la PDN, establece:

"Artículo 50. El sistema estará conformado por los datos resguardados por los encargados, los cuales serán inscritos de acuerdo con las disposiciones establecidas por la Secretaría Ejecutiva en materia de estandarización y distribución; e incluirán, entre otros, las constancias de sanciones o de inhabilitación que se encuentren firmes en contra de los servidores públicos o particulares que hayan sido sancionados por actos vinculados con faltas administrativas graves, la anotación de aquellas abstenciones que hayan realizado las autoridades investigadoras o el Tribunal Federal de Justicia Administrativa en términos de los artículos 77 y 80 de la Ley de Responsabilidades, y la relación de los particulares, personas físicas y morales, que se encuentren inhabilitados para celebrar contratos con los entes públicos derivado de procedimientos administrativos diversos a los previstos por la Ley de Responsabilidades, de conformidad con lo dispuesto en la normativa aplicable."

Por último, es preciso manifestar que, en el mes de febrero del 2019, se publicó en la página de la PDN el estándar de datos para lograr la interoperabilidad con la PDN. El estándar está disponible en: https://plataformadigitalnacional.org/sancionados/especificaciones

Los campos y el diccionario de datos que contiene este sistema se encuentran en:

https://docs.google.com/spreadsheets/d/1wVaVFEJQloanwasIAASFiKGC8mbNEmeiK0F58PxgCA/edit#gid=610045439

[...]

***Artículo 49. La Plataforma Digital Nacional del Sistema Nacional estará conformada por** la información que a ella incorporen las autoridades integrantes del Sistema Nacional y contará, al menos, con los siguientes sistemas electrónicos:*

I y II (...)

III. Sistema nacional de Servidores públicos y particulares sancionados;

(...)"

***"Artículo 52.** El sistema nacional de Servidores públicos y particulares sancionados tiene como finalidad que las sanciones impuestas a Servidores públicos y particulares por la comisión de faltas administrativas en términos de la Ley General de Responsabilidades Administrativas y hechos de corrupción en términos de la legislación penal, queden inscritas dentro del mismo y su consulta deberá estar al alcance de las autoridades cuya competencia lo requiera."*

1. *Artículos 49 a 51 de las Bases para el funcionamiento de la PDN.*

[...]

INFORMACIÓN DEL SISTEMA S6

En términos de lo dispuesto por el artículo 51 de la Ley General del Sistema Nacional Anticorrupción, el Sistema de Información Pública de Contrataciones debe contar con la información pública que remitan las autoridades competentes al Comité Coordinador a solicitud de éste, para el ejercicio de sus funciones y los objetivos de dicha ley.

En cuanto al S6, las Basas para el funcionamiento de la PDN disponen que su objeto es permitir que los distintos usuarios tengan acceso a la información pública de contrataciones, de tal manera qua sea utilizada por los integrantes del Sistema Nacional Anticorrupción en las funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos, y que pueda ser consultada por la ciudadanía en general.

El S6 debe estar conformado por los datos resguardados por los encargados, los cuales serán inscritos de acuerdo con las disposiciones establecidas por la Secretaría Ejecutiva en materia de estandarización y distribución, y deberá contener, al menos, información relacionada con la planeación, los procedimientos de contratación y los datos relevantes y la ejecución de los contratos de adquisiciones, arrendamientos, servicios, obras públicas y servicios relacionados con las mismas.

De igual manera, el sistema inscribirá los datos derivados de manifiesto de vínculos o relaciones de negocios, personales o familiares, así como de posibles conflictos de interés que tengan los particulares, de acuerdo a lo establecido en el protocolo de actuación en contrataciones que al efecto emita el Comité Coordinador de acuerdo a la Ley General de Responsabilidades.
[...]" (Sic)

De igual forma en la atención al requerimiento de información, la SESNA manifestó lo siguiente sobre el principio de licitud:

"[...]

¿Qué es la PDN?:
El desarrollo de la PDN considera seis sistemas que integran datos estratégicos para la lucha contra la corrupción, contemplados en la Ley General del Sistema Nacional Anticorrupción (LGSNA):
- *Sistema 1 Evolución patrimonial, declaración de intereses y constancia de presentación de declaración fiscal (S1).*
- *Sistema 2 Servidores públicos que intervengan en procedimientos de contrataciones públicas (S2).*
- *Sistema 3 Servidores públicos y particulares sancionados (S3).*
- *Sistema 4 Información y comunicación del Sistema Nacional Anticorrupción y el Sistema Nacional de Fiscalización (S4).*
- *Sistema 5 Denuncias por faltas administrativas y hechos de corrupción (S5).*
- *Sistema 6 Información Pública de contrataciones (S6).*

Para entender lo que implica la implementación de la PDN, es importante conocer las atribuciones y competencias de la Secretaría Ejecutiva del Sistema Nacional Anticorrupción:

La responsabilidad de la SESNA es desarrollar y administrar la Plataforma Digital Nacional —en términos del Título Cuarto de la Ley General del Sistema Nacional Anticorrupción (LGSNA) y del Acuerdo mediante el cual el Comité Coordinador del Sistema Nacional Anticorrupción emite el Análisis para la Implementación y Operación de la Plataforma Digital Nacional y las Bases para el Funcionamiento de la Plataforma Digital Nacional (en adelante, Bases), publicado el 23 de octubre del 2018 en el Diario Oficial de la Federación— que de acuerdo con el Artículo 9, es una plataforma que "integre y conecte los diversos sistemas electrónicos que posean datos e información necesaria para que las autoridades competentes tengan Al acceso a los sistemas a que se refiere el Título Cuarto de esta Ley".

De acuerdo con los Artículos 35, fracción X, y 48, párrafo segundo de la LGSNA, la PDN es administrada por la SESNA, a través del Secretario Técnico.

Las Bases emitidas por el Comité Coordinador del Sistema Nacional Anticorrupción, conforme al Artículo 48 de la LGSNA señalan en su Artículo 6, que para el correcto funcionamiento de cada uno de los sistemas, la Secretaría Ejecutiva emitirá los protocolos, estándares, reglamentos, especificaciones técnicas y cualquier normativa necesaria para la colaboración, provisión de datos y acciones para cumplir con las Bases, los cuales serán obligatorios para todos los proveedores, concentradores y encargados a nivel federal, estatal y municipal. Conforme a los Artículos 12, 13, 14 y 15 de las Bases, el desarrollo, mantenimiento y actualización de la PDN forman parte de la administración de la misma.
[...]

Respecto a la información contenida en el Sistema 1, se debe dividir la información en pública y reservada, de acuerdo con lo aprobado por el Comité Coordinador2 -del que forma parte el INAI-. En esta etapa d la PDN solo se cuenta con información de carácter público. Hasta que no se apruebe y publique el catálogo de perfiles -que establecerá quiénes son los usuarios que podrán acceder a la información reservada, conforme a la normativa aplicable- la PDN no permitirá la consulta y el intercambio de los datos reservados. Se aclara que al momento de la presentación de esta Evaluación, este catálogo de perfiles es encuentra en elaboración.2. Los sistemas que se enumeran en el punto dos del requerimiento son sistemas ajenos a la SESNA. Su operación y fundamento son facultades de otras autoridades por lo que la Secretaría está imposibilitada para especificar información o fundamento legal de los mismos. Se mencionaron como ejemplo de fuentes de acceso público donde se encuentra la información pública que, en esta primera etapa, se podrá consultar en la PDN. Esto no significa que sean los únicos sistemas o bases de datos que nutren de información a la PDN, ya que -como el artículo 49 de la LGSNA señala- la Plataforma "estará conformada por la información que a ella incorporen las autoridades integrantes del Sistema Nacional".
[...]

10.La LGSNA establece que el Secretario Técnico será el responsable de "administrar las plataformas digitales que establecerá el Comité Coordinador"12. Además, el Estatuto Orgánico de la SESNA, señala que el titular de la USTPDN está facultado para "implementar, mantener, actualizar y evaluarlos servicios de las plataformas digitales cuya administración son responsabilidad de la Secretaría Ejecutiva"13. Las Bases para el funcionamiento de la PDN establecen:

"Artículo 12. La Plataforma será administrada por la Secretaría Ejecutiva. La administración de la Plataforma implica proveer lo servicios tecnológicos y recursos humanos y financieros necesarios para mantener sus componentes en funcionamiento."

11.L puesta en operación de la PDN es una obligación legal. La LGSNA señala que el Comité Coordinador deberá establecer una Plataforma Digital Nacional con, al menos, los seis sistemas explicados en la Evaluación. El Comité Coordinador es el órgano colegiado facultado para aprobar las bases de su funcionamiento. El INAI forma parte de este órgano colegiado por lo que las decisiones adoptadas cuentan con las observaciones y recomendaciones de esta institución especializada en la protección de datos personales.
[...]" (Sic)

Al respecto, resulta relevante mencionar lo que señala el artículo 113 de la Constitución respecto al SNA:

*"**Artículo 113.** El Sistema Nacional Anticorrupción es la instancia de coordinación entre las autoridades de todos los órdenes de gobierno competentes en la prevención, detección y sanción de responsabilidades administrativas y hechos de corrupción, así como en la fiscalización y control de recursos públicos. Para el cumplimiento de su objeto se sujetará a las siguientes bases mínimas:*

I. El Sistema contará con un Comité Coordinador que estará integrado por los titulares de la Auditoría Superior de la Federación; de la Fiscalía Especializada en Combate a la Corrupción; de la secretaría del Ejecutivo Federal responsable del control interno; por el presidente del Tribunal Federal de Justicia Administrativa; el presidente del organismo garante que establece el artículo 6o. de esta Constitución; así como por un representante del Consejo de la Judicatura Federal y otro del Comité de Participación Ciudadana;
II. El Comité de Participación Ciudadana del Sistema deberá integrarse por cinco ciudadanos que se hayan destacado por su contribución a la transparencia, la rendición de cuentas o el combate a la corrupción y serán designados en los términos que establezca la ley. y
III. Corresponderá al Comité Coordinador del Sistema, en los términos que determine la Ley:
a) El establecimiento de mecanismos de coordinación con los sistemas locales;
b) El diseño y promoción de políticas integrales en materia de fiscalización y control de recursos públicos, de prevención, control y disuasión de faltas administrativas y hechos de corrupción, en especial sobre las causas que los generan;
c) La determinación de los mecanismos de suministro, intercambio, sistematización y actualización de la información que sobre estas materias generen las instituciones competentes de los órdenes de gobierno;
d) El establecimiento de bases y principios para la efectiva coordinación de las autoridades de los órdenes de gobierno en materia de fiscalización y control de los recursos públicos;
e) La elaboración de un informe anual que contenga los avances y resultados del ejercicio de sus funciones y de la aplicación de políticas y programas en la materia.

Derivado de este informe, podrá emitir recomendaciones no vinculantes a las autoridades, con el objeto de que adopten medidas dirigidas al fortalecimiento institucional para la prevención de faltas administrativas y hechos de corrupción, así como el mejoramiento de su desempeño y del control interno. Las autoridades destinatarias de las recomendaciones informarán al Comité sobre la atención que brinden a las mismas.

Las entidades federativas establecerán sistemas locales anticorrupción con el objeto de coordinar a las autoridades locales competentes en la prevención, detección y sanción de responsabilidades administrativas y hechos de corrupción."

Asimismo, conviene traer a colación lo dispuesto en los artículos 8, 9, fracción IX, 48 a 56 de la Ley General del Sistema Nacional, que establecen lo siguiente:

*"**Artículo 8.** El Comité Coordinador es la instancia responsable de establecer mecanismos de coordinación entre los integrantes del Sistema Nacional y tendrá bajo su encargo el diseño, promoción y evaluación de políticas públicas de combate a la corrupción.*

***Artículo 9.** El Comité Coordinador tendrá las siguientes facultades:*

[...]

*IX. **Establecer una Plataforma Digital Nacional** que integre y conecte los diversos sistemas electrónicos que posean datos e información necesaria para que las autoridades competentes tengan acceso a los sistemas a que se refiere el Título Cuarto de esta Ley;*

[...]

***Artículo 48.** El **Comité Coordinador emitirá las bases para el funcionamiento de la Plataforma Digital Nacional** que permita cumplir con los procedimientos, obligaciones y disposiciones señaladas en la presente Ley y la Ley General de Responsabilidades Administrativas, así como para los sujetos de esta Ley, atendiendo a las necesidades de accesibilidad de los usuarios.*

La Plataforma Digital Nacional será administrada por la Secretaría Ejecutiva, a través del Secretario Técnico de la misma, en los términos de esta Ley.

***Artículo 49.** La Plataforma Digital Nacional del Sistema Nacional estará conformada por la información que a ella incorporen las autoridades integrantes del Sistema Nacional y contará, al menos, con los siguientes sistemas electrónicos:*

I. Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal;

II. Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas;

III. Sistema nacional de Servidores públicos y particulares sancionados;

IV. Sistema de información y comunicación del Sistema Nacional y del Sistema Nacional de Fiscalización;

V. Sistema de denuncias públicas de faltas administrativas y hechos de corrupción, y

VI. Sistema de Información Pública de Contrataciones.

***Artículo 50.** Los integrantes del Sistema Nacional y de los Sistemas Locales promoverán la publicación de la información contenida en la plataforma en formato de datos abiertos, conforme a la Ley General de Transparencia y Acceso a la Información Pública y la demás normatividad aplicable.*

El Sistema Nacional establecerá las medidas necesarias para garantizar la estabilidad y seguridad de la plataforma, promoviendo la homologación de procesos y la simplicidad del uso de los sistemas electrónicos por parte de los usuarios.

***Artículo 51.** Los sistemas de evolución patrimonial y de declaración de intereses, así como de los Servidores públicos que intervengan en procedimientos de contrataciones públicas, operarán en los términos de la Ley General de Responsabilidades Administrativas.*

El Sistema de Información Pública de Contrataciones contará con la información pública que remitan las autoridades competentes al Comité Coordinador a solicitud de éste, para el ejercicio de sus funciones y los objetivos de esta Ley.

> ***Artículo 52.*** *El sistema nacional de Servidores públicos y particulares sancionados tiene como finalidad que las sanciones impuestas a Servidores públicos y particulares por la comisión de faltas administrativas en términos de la Ley General de Responsabilidades Administrativas y hechos de corrupción en términos de la legislación penal, queden inscritas dentro del mismo y su consulta deberá estar al alcance de las autoridades cuya competencia lo requiera.*
> ***Artículo 53.*** *Las sanciones impuestas por faltas administrativas graves serán del conocimiento público cuando éstas contengan impedimentos o inhabilitaciones para ser contratados como Servidores públicos o como prestadores de servicios o contratistas del sector público, en términos de la Ley General de Responsabilidades Administrativas.*
> *Los registros de las sanciones relativas a responsabilidades administrativas no graves, quedarán registradas para efectos de eventual reincidencia, pero no serán públicas.*
> ***Artículo 54.*** *El sistema de información y comunicación del Sistema Nacional y del Sistema Nacional de Fiscalización será la herramienta digital que permita centralizar la información de todos los órganos integrantes de los mismos, incluidos los órdenes federal, estatal y, eventualmente, municipal.*
> ***Artículo 55.*** *El sistema de información y comunicación del Sistema Nacional de Fiscalización deberá contemplar, al menos los programas anuales de auditorías de los órganos de fiscalización de los tres órdenes de gobierno; los informes que deben hacerse públicos en términos de las disposiciones jurídicas aplicables, así como la base de datos que permita el adecuado intercambio de información entre los miembros del Sistema Nacional de Fiscalización.*
> *El funcionamiento del sistema de información a que hace alusión el presente artículo se sujetará a las bases que emita el Comité Coordinador respecto a la Plataforma Digital Nacional.*
> ***Artículo 56.*** *El sistema de denuncias públicas de faltas administrativas y hechos de corrupción será establecido de acuerdo a lo que determine el Comité Coordinador y será implementado por las autoridades competentes."*

En virtud de lo anterior, el artículo 113 de la Constitución, señala que el SNA es la instancia de coordinación entre las autoridades de todos los órdenes de gobierno competentes en la prevención, detección y sanción de responsabilidades administrativas y hechos de corrupción, así como en la fiscalización y control de recursos públicos.

Al respecto, se advierte que el SNA cuenta con un Comité Coordinador, que se integra por el titular de la Auditoría Superior de la Federación; el Fiscal Especializado en Combate a la Corrupción; la Secretaría de la Función Pública; el Presidente del Tribunal Federal Justicia Administrativa; el Presidente del Instituto Nacional de Transparencia, Acceso a la Información y protección de Datos Personales; así como por un representante del Consejo de la Judicatura Federal y otro del Comité de Participación Ciudadana.

Asimismo, el artículo constitucional de referencia determinó la creación del Comité de Participación Ciudadana, mismo que se integra por cinco ciudadanos que se hayan destacado por su contribución a la transparencia, la rendición de cuentas o el combate a la corrupción.

En este sentido, de las disposiciones citadas, se advierte que respecto a las atribuciones del Comité Coordinador, **entre ellas se encuentra la de establecer una Plataforma Digital Nacional** que integre y conecte los diversos sistemas electrónicos que posean datos e información necesaria para que las autoridades competentes tengan acceso a los sistemas a que se refiere el Título Cuarto de la misma Ley, siendo el Comité Coordinador **el encargado de emitir las bases para el funcionamiento de la PDN**, administrada por la Secretaría Ejecutiva a través de su Secretario Técnico, que permita cumplir con los procedimientos, obligaciones y disposiciones señaladas tanto en la Ley General del Sistema Nacional como en la Ley General de Responsabilidades.

En este sentido, la PDN, estará conformada por la información que a ella incorporen las autoridades integrantes del Sistema Nacional, establecidas en el artículo 7 de la Ley General del Sistema Nacional, esto es:

1. Los integrantes del Comité Coordinador;
2. El Comité de Participación Ciudadana;
3. El Comité Rector del Sistema Nacional de Fiscalización, y
4. Los Sistemas Locales, quienes concurrirán a través de sus representantes.

La PDN contará, al menos, con los siguientes sistemas electrónicos:

1. Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal;
2. Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas;
3. Sistema nacional de Servidores públicos y particulares sancionados;
4. Sistema de información y comunicación del Sistema Nacional y del Sistema Nacional de Fiscalización;
5. Sistema de denuncias públicas de faltas administrativas y hechos de corrupción, y
6. Sistema de Información Pública de Contrataciones.

Asimismo, se establece que los sistemas de evolución patrimonial y de declaración de intereses, así como de los **Servidores públicos que intervengan en procedimientos de contrataciones públicas**, operarán en los términos de la Ley General de Responsabilidades Administrativas y que el **Sistema de Información Pública de Contrataciones** contará con la información pública que remitan las autoridades competentes al Comité Coordinador.

Aunado a lo anterior, el **sistema nacional de servidores públicos y particulares sancionados** tiene como finalidad que las sanciones impuestas a Servidores públicos y particulares por la comisión de faltas administrativas en términos de la Ley General de Responsabilidades Administrativas y hechos

de corrupción en términos de la legislación penal queden inscritas dentro del mismo y su consulta deberá estar al alcance de las autoridades cuya competencia lo requiera.

En relación con lo anterior, el Comité Coordinador emitió las Bases para el funcionamiento de la Plataforma Digital Nacional, que tienen por objeto establecer las directrices para el funcionamiento de la PDN y los sistemas que la conforman, que garanticen la interoperabilidad, interconexión, estabilidad, uso y seguridad de la información integrada en la Plataforma, promover la homologación de procesos, estandarización de datos y la simplicidad del uso para los usuarios; teniendo en cuenta en todo momento los derechos de acceso a la información y protección de datos personales en posesión de los sujetos obligados; que permitan cumplir con los procedimientos, obligaciones y disposiciones del Sistema Nacional Anticorrupción y las instituciones que lo conforman.

En este sentido, el artículo 12 de las mencionadas Bases para el funcionamiento de la PDN, en concordancia con lo señalado en el artículo 48 de la Ley General del Sistema Nacional, establecen que la **PND será administrada por la SESNA**, a través del Secretario Técnico de la misma, en los términos de la misma Ley, lo cual implica que tendrá la obligación de:

- Proveer los servicios tecnológicos y recursos humanos y financieros necesarios para mantener sus componentes en funcionamiento.
- Verificar de manera permanente el correcto funcionamiento de los componentes de la PDN y sus sistemas, con la finalidad de prevenir fallas y, en caso de diagnosticarlas, dar pronta atención a las mismas.
- Asegurar que los usuarios tengan acceso a la Plataforma.
- Vigilar y dar cuenta de su correcto funcionamiento al Comité Coordinador.
- En caso de que la Plataforma o alguno de sus sistemas presente una falla técnica, hacer del conocimiento de los usuarios la magnitud de la falla y el tiempo de recuperación, para que éstos estén en posibilidad de implementar las medidas necesarias para el cumplimiento de sus respectivas obligaciones.
- Asimismo, en caso de que algún subsistema o conjunto de datos presente una falla técnica, el encargado o concentrador correspondiente deberá hacer del conocimiento de la Secretaría Ejecutiva la magnitud de la falla y el tiempo de recuperación, para que la Secretaría Ejecutiva esté en posibilidad de implementar las medidas necesarias para el cumplimiento de sus respectivas obligaciones en tiempo y forma.
- Informar bimestralmente a los integrantes del Comité Coordinador sobre el funcionamiento de la Plataforma, recomendaciones para mejorarlo, y sobre las fallas que éstas o cualquiera de sus componentes puedan haber presentado, y las medidas que se tomarán para solucionarlas.

Al respecto, los diferentes usuarios de la PDN podrán consultar la información dentro de cada uno de los sistemas de información, para las diferentes funcionalidades y alcances de acuerdo con cada perfil, a través de la conexión con diferentes fuentes de origen a saber:

- Con un ecosistema federal que incluya el conjunto de datos que generarán las entidades públicas a nivel federal, es decir, los Poderes Ejecutivo, Legislativo y Judicial, por los Órganos Constitucionalmente Autónomos, así como por las Empresas Productivas del Estado, y por cualquier otra entidad con naturaleza diferente a éstas que opere a nivel federal.
- Simultáneamente cada uno de los sistemas de la PDN deberá conectarse con los conjuntos de datos que hay en cada una de las 32 Entidades Federativas. Se deberá contemplar que cada Sistema Local Anticorrupción deberá contar con ese espejo de la PDN que contenga la información que se genera en cada Entidad Federativa, y que, a través de cada Secretaría Ejecutiva de los Sistemas Locales, se concentrará y conectará la información con la PDN.

Asimismo, con la puesta en operación de la PDN, se busca como finalidad de manera general el contar con una plataforma que integre y conecte los diversos sistemas electrónicos que posean datos e información necesaria para que las autoridades competentes tengan acceso a los 6 sistemas a que se refiere el Título Cuarto de la Ley General del Sistema Nacional:

1. Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal;
2. Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas;
3. Sistema nacional de Servidores públicos y particulares sancionados;
4. Sistema de información y comunicación del Sistema Nacional y del Sistema Nacional de Fiscalización;
5. Sistema de denuncias públicas de faltas administrativas y hechos de corrupción, y
6. Sistema de Información Pública de Contrataciones.

Lo anterior, para cumplir a su vez con los siguientes objetivos:

- Contar con una fuente de **inteligencia para construir integridad y combatir la corrupción,** que creará valor para el gobierno y la sociedad, a partir de grandes cantidades de datos.
- Un **medio para el intercambio de datos anticorrupción**, que busca quitar barreras y romper silos de información para que los datos sean comparables, accesibles y utilizables, empezando con **seis sistemas de datos prioritarios**, **interoperables**, **estandarizados y distribuidos para ser consultados desde la Plataforma**.

- Hacer interoperable la información a fin de permitir **el intercambio y consulta de datos eficiente** con autoridades y ciudadanía, cuidando en todo momento la seguridad e integridad de la información.

Asimismo, mediante el uso de **nuevas tecnologías, metodologías de trabajo, ciencia de datos e inteligencia artificial** como insumos y apoyo al trabajo de las autoridades del **SNA** para:

- **Analizar, predecir y alertar** a las autoridades sobre posibles riesgos de corrupción.
- **Automatizar procesos, evitar discrecionalidad, colusión y conflicto de interés.**
- **Promover el uso de los datos** para respaldar sanciones y como evidencia para combatir la impunidad.
- **Dar seguimiento, en tiempo real**, a los procesos y proyectos de contratación pública, asegurar el cumplimiento de sus objetivos y garantizar una mayor eficiencia en las compras públicas.
- **Apoyar la participación ciudadana**, poniendo al ciudadano al centro del combate a la corrupción.
- **Incorporar información sobre indicadores** para evaluar la Política Nacional Anticorrupción y el fenómeno en México.
- **Dar evidencia para generar recomendaciones de política pública** a las autoridades del Sistema Naciona Anticorrupción.

Aunado a lo anterior, la Plataforma deberá contemplar la exportación de información por parte de los usuarios, de conformidad con el acceso determinado en el catálogo de perfiles. El uso de la información será responsabilidad de cada usuario, de conformidad con la normativa aplicable.

Por lo cual, el Instituto determina que el tratamiento de datos personales que llevará a cabo la SESNA a través de la puesta en operación de la PDN encuentra su fundamento en los artículos 113 de la Constitución Política de los Estados Unidos Mexicanos, 8 y 9 fracción IX, 48 a 56 de la Ley General del Sistema Nacional Anticorrupción, así como en las Bases para el funcionamiento de la PDN, emitidas por el Comité Coordinador del SNA.

En este sentido, la Plataforma Digital Nacional cumple con el principio de licitud a que se refieren los artículos 17 de la Ley General y 8 de los Lineamientos Generales, en el entendido de que todo tratamiento de datos personales debe realizarse con estricto apego a la legislación mexicana y, en su caso, al derecho internacional que resulte aplicable, así como a las atribuciones conferidas al responsable por la normatividad que resulte aplicable.

1.2 Principio de finalidad

El artículo 18 de la Ley General establece lo siguiente:

> "***Artículo 18.*** *Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.*
>
> *El responsable podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia."*

Por su parte, los artículos 9 y 10 de los Lineamientos generales indican:

> "***Principio de finalidad***
> ***Artículo 9.*** *Para efectos de lo previsto en el artículo 18, primer párrafo de la Ley General y los presentes Lineamientos generales se entenderá que las finalidades son:*
>
> *I. Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que se admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.*
> *II. Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad;*
> *III. Lícitas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y el derecho internacional que le resulte aplicable, y*
> *IV. Legítimas: cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.*
>
> ***Tratamiento para finalidades distintas***
> ***Artículo 10.*** *En el tratamiento de datos personales para finalidades distintas a aquellas que motivaron su tratamiento original a que se refiere el artículo 18, segundo párrafo de la Ley General, el responsable deberá considerar:*
>
> *I. La expectativa razonable de privacidad del titular basada en la relación que tiene con éste;*
> *II. La naturaleza de los datos personales;*
> *III. Las consecuencias del tratamiento posterior de los datos personales para el titular, y*
> *IV. Las medidas adoptadas para que el tratamiento posterior de los datos personales cumpla con las disposiciones previstas en la Ley General y los presentes Lineamientos generales."*

De lo anterior, se desprende que el responsable tiene la obligación de definir las finalidades concretas, lícitas, explícitas y legítimas a que serán sometidos los datos personales para cumplir con los objetivos que persigue, los cuales, en todo momento, deberán ser acordes con las atribuciones que la normatividad aplicable le confiera a éste.

Se entenderá que las finalidades son:

- Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados, sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión en el titular.
- Explícitas: cuando las finalidades se expresan y dan a conocer de manera clara en el aviso de privacidad.
- Lícitas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y, en su caso, el derecho internacional que le resulte aplicable.
- Legítimas: cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General.

En caso de que el responsable pretendiera tratar los datos personales para finalidades distintas a las originalmente previstas, podrá hacerlo siempre y cuando cuente con atribuciones conferidas en la ley y solicite el consentimiento del titular.

Sobre el particular, en la presentación de la evaluación de impacto en la protección de datos personales, la SESNA manifestó lo siguiente:

"[...]

S1.

"II. 3 finalidades concretas, lícitas, explícitas y legítimas del S1.

El S1 tiene como objeto permitir la consulta de los datos de los servidores públicos obligados a presentar declaración patrimonial y de intereses, así como de garantizar la inscripción de la constancia de la declaración anual de impuestos que emita la autoridad fiscal competente.11 con las siguientes finalidades:

***1.** Que la información del sistema pueda ser solicitada y utilizada de acuerdo con las necesidades de las diversas autoridades competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción, entre las que se encuentran el Ministerio Público, Tribunales o autoridades judiciales, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras, entre otras;*

***2.** En una sola plataforma informática, dar acceso al público en general a la información pública de las declaraciones del S1 conforme a las disposiciones y normas de operación aprobadas por el Comité Coordinador, mediante el "ACUERDO por el que se modifican los Anexos Primero y Segundo del Acuerdo por el que el Comité Coordinador del Sistema Nacional Anticorrupción emite el formato de declaraciones: de situación patrimonial y de intereses; y expide las normas e instructivo para su llenado y presentación", publicado en el Diario Oficial de la Federación el 23 de septiembre de 2019;*

3. Permitir que la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos, realicen la verificación aleatoria de las declaraciones y patrimonial, de intereses y fiscal, para identificar la evolución del patrimonio de los servidores públicos, y
4. Expedición de certificaciones de la inexistencia de anomalías de las declaraciones presentadas por los servidores públicos que obran en el S1."

S2
"III.3 Finalidades concretas, lícitas, explícitas y legítimas.
El S2 tiene como objeto permitir que el público en general usuarios tenga acceso a la información relacionada con los servidores públicos que intervienen en procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, de tal manera que sea utilizada por los integrantes del Sistema Nacional Anticorrupción y autoridades competentes en la prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.[16]
Así las cosas, la finalidad principal del tratamiento de datos personales del S2 consiste en que las autoridades competentes de los tres órdenes de gobierno para prevenir, detectar, investigar y sancionar faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos, tengan acceso a, por lo menos, los nombres y adscripción de los servidores públicos que intervienen en procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, para ejercer sus facultades."

S3
IV.3 Finalidades concretas, lícitas, explícitas y legítimas.
Con fundamento en el artículo 52 de la Ley General del Sistema Nacional Anticorrupción, el S3 tiene como finalidad que las sanciones impuestas a servidores públicos y particulares por la comisión de faltas administrativas graves en términos de la Ley General de Responsabilidades Administrativas y hechos de corrupción en términos de la legislación penal, queden inscritas y su consulta esté al alcance de los Entes públicos del estado mexicano que lo requieran.

Lo anterior, para que los Entes públicos del estado mexicano, previo al nombramiento, designación o contratación de las personas que pretendan ingresar al servicio público, consulten el Sistema Nacional de Servidores Públicos y Particulares Sancionados de la Plataforma Digital Nacional, con el fin de verificar que no estén inhabilitados por la comisión de faltas graves en los términos dispuestos por las leyes en materia de responsabilidades administrativas o hechos de corrupción en términos de la legislación penal, en cuyo caso, se abstendrán de realizar el nombramiento, designación o contratación respectiva.

S6
"V.3 Finalidades concretas, lícitas, explícitas y legítimas.

Contar con un sistema de consulta pública, que permita a sus usuarios, Entes públicos y ciudadanos, realizar la de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.

[...]" (Sic)

Adicionalmente, en su respuesta al requerimiento de información adicional, la SESNA manifestó que:

"[...]

En primer lugar, se aclara que no existe un cambio en las finalidades que justifican el origen del tratamiento de datos personales que conforman los sistemas 1, 2, 3 y 6. La Ley General de Responsabilidades Administrativas expresamente señala que "la información relacionada con las declaraciones de situación patrimonial y de intereses, podrá ser solicitada y utilizada por el Ministerio Público, los Tribunales o las autoridades judiciales en el ejercicio de sus respectivas atribuciones, el Servidor Público interesado o bien, cuando las Autoridades investigadoras, substanciadoras o resolutoras lo requieran con motivo de la investigación o la resolución de procedimientos de responsabilidades administrativas".

Adicionalmente, las Bases aprobadas por el Comité Coordinador -del que el INAI forma parte- también establecen la posibilidad de esta transferencia de información con el objetivo de investigar y sancionar posibles faltas administrativas o delitos de corrupción. Se reitera que, como lo establecen las Bases de la PDN en su Artículo 27,: "Artículo 27. La Plataforma deberá contemplar la exportación de información por parte de los usuarios, de conformidad con el acceso determinado en el catálogo de perfiles. El uso de la información será responsabilidad de cada usuario, de conformidad con la normativa aplicable "Los catálogos de perfiles no han sido aprobados por el Comité Coordinador por lo que actualmente no se encuentran definidas las funcionalidades de acuerdo con el perfil.
[...]

De acuerdo con las Bases, la SESNA deberá emitir un mecanismo que permita a las Secretarías y Órganos Internos de Control realizar la verificación aleatoria de las declaraciones patrimonial, de intereses y para identificar la evolución del patrimonio de los servidores públicos. También emitirá un mecanismo para la expedición de certificaciones de la inexistencia de anomalías que deberán anotarse en el Sistema 1. Ambos mecanismos se encuentran en proceso de elaboración.

7. La PDN no recaba datos personales ya que es una plataforma de interoperabilidad que opera con una arquitectura basada en comunicaciones a través de Internet, que permite consultar información desde diversos proveedores de información (Entes públicos), en tiempo real y de manera estandarizada (en un mismo formato). Esto está establecido en las Bases de la Plataforma Digital Nacional (artículos 7,8,9,10 y 11) [...]

La LGSNA9 establece que la Plataforma estará conformada por la información que a ella incorporen las autoridades integrantes del Sistema Nacional y contará, al menos, con los 6 sistemas que se señalaron en la Evaluación. Esto significa que, de acuerdo a las Bases de la PDN, cada Encargado y Concentrador, será responsable de recabar la información y generar los esquemas necesarios para conectarse con la PDN.
[...]

Será responsabilidad de ellos designar a los responsables de los sistemas fuentes de información que proveerán y actualizarán los sistemas 1, 2, 3 y 6.

8. Como se señaló en la Evaluación, la información contenida en el S1 es susceptible de ser transferida a las diversas autoridades de los tres órdenes de gobierno, competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción, entre las que se encuentran el Ministerio Público, órganos jurisdiccionales como el Tribunal Federal de Justicia Administrativa y sus homólogos en las entidades federativas, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras a las que alude la LGRA, como la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos.

El artículo 28 de la LGRA habilita esta transferencia con la finalidad de apoyar en "la investigación o la resolución de procedimientos de responsabilidades administrativas". La información contenida en el Sistema 1 se captura a través de los formatos aprobados por el Comité Coordinador. Estos tienen dos apartados, el público y el reservado. En cumplimiento de lo acordado por el Comité Coordinador, el apartado público podrá ser consultado por cualquier ciudadano a través de la PDN. El componente reservado únicamente podrá tener acceso aquellos funcionarios con la facultad legal de hacerlo. El funcionario que tenga los permisos necesarios para acceder a esta información reservada podrá consultar todos los datos personales contenidos en los formatos aprobados por el Comité Coordinador11. En este momento únicamente se podrá acceder al componente público del Sistema 1 ya que no se ha publicado el catálogo de perfiles.

9. La PDN es una herramienta creada en la LGSNA y no está condicionada a un tiempo de duración, su funcionamiento permanecerá activo siempre que exista el Sistema Nacional Anticorrupción y la SESNA como institución encargada de su administración. Como se señaló en la evaluación, la PDN es una plataforma de interoperabilidad por lo que no genera ni almacena los datos. A través de servicios web o API`s, consulta la información de los servidores y las bases de datos de los generadores de la información, y los refleja en la Plataforma. Una API es un conjunto de definiciones y protocolos que se utiliza para desarrollar e integrar el software de las aplicaciones. Las API permiten que sus productos y servicios se comuniquen con otros, sin necesidad de saber cómo están implementados. La PDN no se encuentra permanentemente conectada a los sistemas sino que se activa el canal de comunicación (API) en cada consulta.
[...]" (Sic)

Ahora bien, retomando lo dispuesto en el Título Cuarto de la Ley General del Sistema Nacional, así como de las Bases para el funcionamiento de la PND, la SESNA cuenta con las atribuciones para administrar la PDN, a través de su Secretario Técnico, así como para establecer las medidas necesarias para garantizar la estabilidad y seguridad de la plataforma, promoviendo la homologación de procesos y la simplicidad del uso de los sistemas electrónicos por parte de los usuarios.

Concretamente, la SESNA cuenta con atribuciones para:

- Proveer los servicios tecnológicos y recursos humanos y financieros necesarios para mantener sus componentes en funcionamiento.

- Verificar de manera permanente el correcto funcionamiento de los componentes de la PDN y sus sistemas, con la finalidad de prevenir fallas y, en caso de diagnosticarlas, dar pronta atención a las mismas.
- Asegurar que los usuarios tengan acceso a la Plataforma.
- Vigilar y dar cuenta de su correcto funcionamiento al Comité Coordinador.
- En caso de que la Plataforma o alguno de sus sistemas presente una falla técnica, hacer del conocimiento de los usuarios la magnitud de la falla y el tiempo de recuperación, para que éstos estén en posibilidad de implementar las medidas necesarias para el cumplimiento de sus respectivas obligaciones.
- Asimismo, en caso de que algún subsistema o conjunto de datos presente una falla técnica, el encargado o concentrador correspondiente deberá hacer del conocimiento de la Secretaría Ejecutiva la magnitud de la falla y el tiempo de recuperación, para que la Secretaría Ejecutiva esté en posibilidad de implementar las medidas necesarias para el cumplimiento de sus respectivas obligaciones en tiempo y forma.
- Informar bimestralmente a los integrantes del Comité Coordinador sobre el funcionamiento de la Plataforma, recomendaciones para mejorarlo, y sobre las fallas que ésta o cualquiera de sus componentes puedan haber presentado, y las medidas que se tomarán paras solucionarlas.

Bajo esta tesitura, se advierte que el tratamiento de datos personales que se llevará a cabo a través de **la PDN** será utilizado para el desempeño de las atribuciones y funciones que le han sido conferidas a la SESNA.

En este sentido, se advierte que el tratamiento de datos personales que se llevará a cabo a través de la PDN y los sistemas que la conforman tiene como finalidad el cumplimiento de las siguientes finalidades:

- La interoperabilidad, interconexión, estabilidad, uso y seguridad de la información integrada en la Plataforma, esto es, contar con una plataforma que integre y conecte los diversos sistemas electrónicos que posean datos e información necesaria para que las autoridades competentes tengan acceso a los 6 sistemas a que se refiere el Título Cuarto de la Ley General del Sistema Nacional:
    1. Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal;
    2. Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas;
    3. Sistema nacional de Servidores públicos y particulares sancionados;

4. Sistema de información y comunicación del Sistema Nacional y del Sistema Nacional de Fiscalización;
5. Sistema de denuncias públicas de faltas administrativas y hechos de corrupción, y
6. Sistema de Información Pública de Contrataciones.

- Promover la homologación de procesos, estandarización de datos y la simplicidad del uso para los usuarios.
- Tener en cuenta en todo momento los derechos de acceso a la información y protección de datos personales en posesión de los sujetos obligados; que permitan cumplir con los procedimientos, obligaciones y disposiciones del Sistema Nacional Anticorrupción y las instituciones que lo conforman.
- Que los diferentes usuarios de la PDN puedan consultar la información dentro de cada uno de los sistemas de información, para las diferentes funcionalidades y alcances de acuerdo con cada perfil, a través de la conexión con diferentes fuentes de origen a saber:
  - Con un ecosistema federal que incluya el conjunto de datos que generarán las entidades públicas a nivel federal, es decir, los Poderes Ejecutivo, Legislativo y Judicial, por los Órganos Constitucionalmente Autónomos, así como por las Empresas Productivas del Estado, y por cualquier otra entidad con naturaleza diferente a éstas que opere a nivel federal.
  - Simultáneamente cada uno de los sistemas de la PDN deberá conectarse con los conjuntos de datos que hay en cada una de las 32 Entidades Federativas. Se deberá contemplar que cada Sistema Local Anticorrupción deberá contar con ese espejo de la PDN que contenga la información que se genera en cada Entidad Federativa, y que, a través de cada Secretaría Ejecutiva de los Sistemas Locales, se concentrará y conectará la información con la PDN.
- Contar con una fuente de **inteligencia para construir integridad y combatir la corrupción,** que creará valor para el gobierno y la sociedad, a partir de grandes cantidades de datos.
- Un **medio para el intercambio de datos anticorrupción**, que busca quitar barreras y romper silos de información para que los datos sean comparables, accesibles y utilizables, empezando con **seis sistemas de datos prioritarios**, **interoperables**, **estandarizados y distribuidos para ser consultados desde la Plataforma**.
- Permitir **el intercambio y consulta de datos eficiente** con autoridades y ciudadanía, cuidando en todo momento la seguridad e integridad de la información.

Asimismo, mediante el uso de **nuevas tecnologías, metodologías de trabajo, ciencia de datos e inteligencia artificial** como insumos y apoyo al trabajo de las autoridades del **SNA** para:

- **Analizar, predecir y alertar** a las autoridades sobre posibles riesgos de corrupción.

- **Automatizar procesos, evitar discrecionalidad, colusión y conflicto de interés.**
- **Promover el uso de los datos** para respaldar sanciones y como evidencia para combatir la impunidad.
- **Dar seguimiento, en tiempo real**, a los procesos y proyectos de contratación pública, asegurar el cumplimiento de sus objetivos y garantizar una mayor eficiencia en las compras públicas.
- **Apoyar la participación ciudadana**, poniendo al ciudadano al centro del combate a la corrupción.
- **Incorporar información sobre indicadores** para evaluar la Política Nacional Anticorrupción y el fenómeno en México.
- **Dar evidencia para generar recomendaciones de política pública** a las autoridades del Sistema Nacional Anticorrupción.

Asimismo, cabe señalar que la PDN **asegurará la interoperabilidad de la información que se conecte e integre, así como la que se genere, en cada sistema y entre los diversos sistemas.** Además, deberá contemplar la exportación de información por parte de los usuarios, de conformidad con el acceso determinado en el catálogo de perfiles que el uso de la información será responsabilidad de cada usuario, de conformidad con la normativa aplicable.

Al respecto, cabe señalar que cada uno de los sistemas que la conforman, mismos que se refieren como objeto de la presente evaluación de impacto, esto es los sistemas S1, S2, S3 y S6 a su vez, tienen finalidades especificas, a saber:

S1. OBJETO DEL SISTEMA DE EVOLUCIÓN PATRIMONIAL, DE DECLARACIÓN DE INTERESES Y CONSTANCIA DE PRESENTACIÓN DE DECLARACIÓN FISCAL:

- La SESNA deberá establecer los mecanismos para que la información del sistema sea solicitada y utilizada de acuerdo con las necesidades de las diversas autoridades competentes, entre las que se encuentran el Ministerio Público, Tribunales o autoridades judiciales, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras, entre otras, en el ejercicio de sus respectivas atribuciones y de conformidad con la normativa aplicable, previa aprobación del Comité Coordinador.
- La SESNA establecerá un portal del sistema para dar acceso a la información pública de las declaraciones conforme a las disposiciones y normas de operación aprobadas por el Comité Coordinador.
- La SENSA deberá establecer un mecanismo que permita que las Secretarias y Órganos Internos de Control realicen la verificación aleatoria de las declaraciones patrimonial, de intereses, y para identificar la evolución del patrimonio de los servidores públicos.

- La Secretaría Ejecutiva deberá establecer un mecanismo para la expedición de certificaciones de la inexistencia de anomalías, las cuales deberán anotarse en el sistema. Asimismo, en caso de la detección de anomalías, el sistema contemplará un mecanismo para dar inicio a la investigación correspondiente.

S2. SISTEMA DE LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN PROCEDIMIENTOS DE CONTRATACIONES PÚBLICAS:

- El objeto del sistema es permitir que los distintos usuarios tengan acceso a la información relacionada con los servidores públicos que intervienen en procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, de tal manera que sea utilizada por los integrantes del Sistema Nacional Anticorrupción y autoridades competentes en sus funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.
- El sistema estará conformado por los datos resguardados por los encargados, de acuerdo con los formatos especificados por el Comité Coordinador. Estos datos deberán ser actualizados de manera quincenal por los entes e incluirán, como mínimo, los nombres y adscripción de los servidores públicos que intervengan en contrataciones, así como la relación de particulares, personas físicas y morales que se encuentren inhabilitados para celebrar contratos con los entes públicos, derivado de procedimientos administrativos diversos a los previstos en la Ley de Responsabilidades.
- La Secretaría Ejecutiva establecerá un portal de internet, a través del cual se ponga a disposición de todo público los datos públicos a que se refiere el presente capítulo.

S3. DEL SISTEMA NACIONAL DE SERVIDORES PÚBLICOS Y PARTICULARES SANCIONADOS:

- Este sistema tiene como objeto permitir que los usuarios tengan acceso a los datos relacionados con sanciones impuestas a servidores públicos y particulares por la comisión de faltas administrativas, en términos de la Ley de Responsabilidades, y hechos de corrupción, en términos de la legislación penal aplicable, a fin de hacer disponible dicha información para las autoridades cuya competencia lo requiera.
- El sistema estará conformado por los datos resguardados por los encargados, los cuales serán inscritos de acuerdo con las disposiciones establecidas por la Secretaría Ejecutiva en materia de estandarización y distribución; e incluirán, entre otros, las constancias de sanciones o de inhabilitación que se encuentren firmes en contra de los servidores públicos o

particulares que hayan sido sancionados por actos vinculados con faltas administrativas graves, la anotación de aquellas abstenciones que hayan realizado las autoridades investigadoras o el Tribunal Federal de Justicia Administrativa en términos de los artículos 77 y 80 de la Ley de Responsabilidades, y la relación de los particulares, personas físicas y morales, que se encuentren inhabilitados para celebrar contratos con los entes públicos derivado de procedimientos administrativos diversos a los previstos por la Ley de Responsabilidades, de conformidad con lo dispuesto en la normativa aplicable.

- Respecto de la información relacionada con las sanciones impuestas por la comisión de hechos de corrupción, se atenderá a lo dispuesto en la legislación penal y procesal penal aplicable, así como a la normativa que para el efecto establezca la Fiscalía Especializada en Combate a la Corrupción y el Poder Judicial de la Federación.
- La Secretaría Ejecutiva establecerá un portal para dar acceso a la información pública de este sistema. Las sanciones impuestas por faltas administrativas graves serán del conocimiento público cuando éstas impliquen impedimentos o inhabilitaciones a personas para ser contratadas como servidores públicos, como prestadores de servicios o contratistas del sector público, en términos de la Ley de Responsabilidades. Los registros de las sanciones relativas a responsabilidades administrativas no graves quedarán inscritos para efectos de ser consideradas en el caso de eventuales reincidencias, pero no serán públicos.

S6. DEL SISTEMA DE INFORMACIÓN PÚBLICA DE CONTRATACIONES:

- El objeto del sistema es permitir que los distintos usuarios tengan acceso a la información pública de contrataciones, de tal manera que sea utilizada por los integrantes del Sistema Nacional Anticorrupción en las funciones de prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos, y que pueda ser consultada por la ciudadanía en general.
- El sistema estará conformado por los datos resguardados por los encargados, los cuales serán inscritos de acuerdo con las disposiciones establecidas por la Secretaría Ejecutiva en materia de estandarización y distribución, y deberá contener, al menos, información relacionada con la planeación, los procedimientos de contratación y los datos relevantes y la ejecución de los contratos de adquisiciones, arrendamientos, servicios, obras públicas y servicios relacionados con las mismas.
- De igual manera, el sistema inscribirá los datos derivados del manifiesto de vínculos o relaciones de negocios, personales o familiares, así como de posibles conflictos de interés que tengan los particulares, de acuerdo con lo establecido en el protocolo de actuación en contrataciones emitido por el Comité Coordinador de acuerdo con la Ley de Responsabilidades. La Secretaría Ejecutiva establecerá un portal para dar acceso a la

información agregada de este sistema, para lo cual deberá atender, preferentemente, al Estándar de Datos para Contrataciones Abiertas.

Cabe resaltar, que adicionalmente, posteriormente se integrarán a la PDN el Sistema de información y comunicación del Sistema Nacional Anticorrupción y del Sistema nacional de fiscalización y de denuncias públicas de faltas administrativas y hechos de corrupción, así como sistemas adicionales a propuesta de uno o más miembros del Comité Coordinador, y previo dictamen técnico de la Secretaría Ejecutiva.

De las consideraciones anteriores, el Instituto determina que las finalidades que justifican el tratamiento de datos personales que se llevará a cabo a través de la PDN, se caracterizan por ser concretas, debido a que las finalidades generales de la conformación de la plataforma se materializan en fines específicos, relacionados con cada uno de los sistemas que la conforman.

Asimismo, las finalidades descritas resultan lícitas, toda vez que son acordes con lo establecido en el Capítulo Cuarto de la Ley General del Sistema Nacional, así como en las Bases para el funcionamiento de la PDN, en relación con las atribuciones y facultades que le son conferidas a la SESNA en relación con la administración y operación de la plataforma.

Con relación a que las finalidades que motivan el tratamiento de los datos personales cumplan con el requisito de ser legítimas, conviene manifestar que está característica se actualizará en la medida de que las comunicaciones de datos personales que realicen los entes públicos para integrar los sistemas que conforman el PDN **estén habilitadas por el consentimiento del titular**, cuando éste sea exigible, o bien, por la actualización de una causal de excepción conforme a la legislación en la materia que resulte aplicable.

Al respecto, se observa que la obligación de obtener el consentimiento de los titulares para el tratamiento de sus datos personales, corresponderá a los proveedores de información (entes públicos), con atribuciones en la materia, siempre y cuando el consentimiento sea exigible en términos de la normatividad de protección de datos personales que resulte aplicable a dichos entes públicos en función de su naturaleza pública de carácter federal, estatal o municipal, consideraciones que serán analizadas bajo el principio de consentimiento.

Por último, en la determinación si las finalidades que justificarán el tratamiento de los datos personales que se llevara a cabo a través de la PDN, son explícitas, este Instituto hace propias las consideraciones señaladas en el principio de información.

Conforme lo anterior, se concluye que la SESNA cumple con el principio de finalidad a que se refieren los artículos 18 de la Ley General y 9 de los Lineamientos generales en el sentido de que todo tratamiento de datos personales debe estar justificado por finalidades concretas, explícitas, lícitas y legítimas acorde con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación mexicana y, en su caso, el derecho internacional que resulte aplicable.

1.3 Principio de lealtad

El artículo 19 de la Ley General establece lo siguiente:

> *"**Artículo 19.** El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad."*

Por su parte, el artículo 11 de los Lineamientos generales señala lo siguiente:

> *"**Principio de lealtad***
> ***Artículo 11.** En términos de lo dispuesto en el artículo 19 de la Ley General y los presentes Lineamientos generales, se entenderá:*
> *I. Por medios engañosos o fraudulentos aquellos que el responsable utilice para tratar los datos personales con dolo, mala fe o negligencia;*
> *II. Que el responsable privilegia los intereses del titular cuando el tratamiento de datos personales que efectúa no da lugar a una discriminación o trato injusto o arbitrario contra éste, y*
> *III. Por expectativa razonable de privacidad, la confianza que el titular ha depositado en el responsable respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la Ley General y los presentes Lineamientos generales." (Sic).*

De lo anterior, este Instituto observa que el responsable no debe actuar de manera engañosa o fraudulenta respecto al tratamiento de los datos personales que lleve a cabo, para lo cual se entiende:

- Por medios engañosos o fraudulentos: aquéllos que el responsable utilice para tratar los datos personales con dolo, mala fe o negligencia.
- Que el responsable privilegia los intereses del titular: cuando el tratamiento de datos personales que efectúa no da lugar a una discriminación o trato injusto o arbitrario contra éste.
- Por expectativa razonable de privacidad: la confianza que el titular ha depositado en el responsable respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento a las disposiciones previstas en la Ley General y los Lineamientos generales.

Al respecto, la SESNA manifestó lo siguiente:

"[...]

La responsabilidad de la SESNA es desarrollar y administrar la Plataforma Digital Nacional —en términos del Título Cuarto de la Ley General del Sistema Nacional Anticorrupción (LGSNA) y del Acuerdo mediante el cual el Comité Coordinador del Sistema Nacional Anticorrupción emite el Análisis para la Implementación y Operación de la Plataforma Digital Nacional y las Bases para el Funcionamiento de la Plataforma Digital Nacional (en adelante, Bases), publicado el 23 de octubre del 2018 en el Diario Oficial de la Federación— que de acuerdo con el Artículo 9, es una plataforma que "integre y conecte los diversos sistemas electrónicos que posean datos e información necesaria para que las autoridades competentes tengan acceso a los sistemas a que se refiere el Título Cuarto de esta Ley".

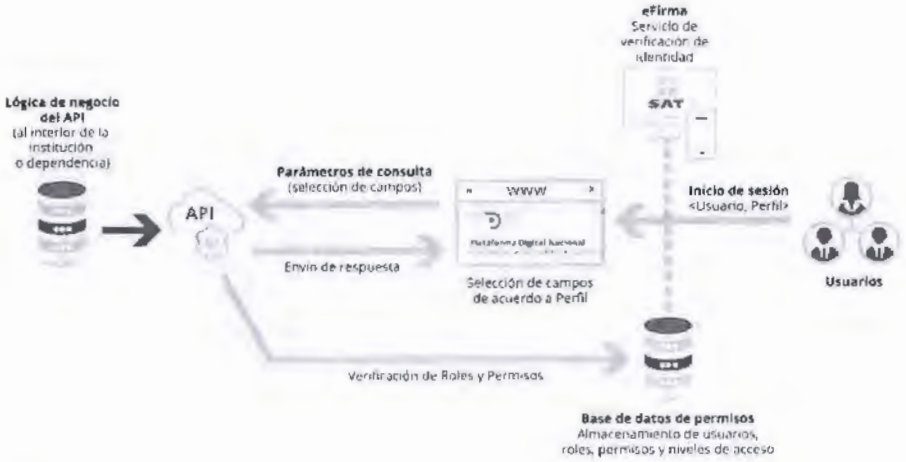
De acuerdo con los Artículos 35, fracción X, y 48, párrafo segundo de la LGSNA, la PDN es administrada por la SESNA, a través del Secretario Técnico. Las Bases emitidas por el Comité Coordinador del Sistema Nacional Anticorrupción, conforme al Artículo 48 de la LGSNA señalan en su Artículo 6, que para el correcto funcionamiento de cada uno de los sistemas, la Secretaría Ejecutiva emitirá los protocolos, estándares, reglamentos, especificaciones técnicas y cualquier normativa necesaria para la colaboración, provisión de datos y acciones para cumplir con las Bases, los cuales serán obligatorios para todos los proveedores, concentradores y encargados a nivel federal, estatal y municipal.

Conforme a los Artículos 12, 13, 14 y 15 de las Bases, el desarrollo, mantenimiento y actualización de la PDN forman parte de la administración de la misma. Al ser una plataforma de interoperabilidad, la PDN no genera ni almacena los datos, sino que a través de servicios web o API's, consulta la información de los servidores y las bases de datos de los generadores de la información, y los refleja en la Plataforma.

[...]
La PDN opera con una arquitectura basada en comunicaciones a través de internet, que permite consultar información desde diversos proveedores de información (entes de gobierno), en tiempo real y de manera estandarizada (en un mismo formato). Con el objetivo de incorporar datos a la PDN, los generadores de información deben establecer mecanismos tecnológicos que permitan la consulta de información desde la PDN hacia sus bases de datos. La SESNA publicó las ***Especificaciones Técnicas*** *y* ***Estándares de Datos*** *que permiten que cualquier ente del gobierno pueda desarrollar los mecanismos de comunicación.*
[...]" (Sic)

Asimismo, a continuación, se señala el flujo de la operación de **la PDN:**

"[...]



[...]" *(Sic)*

A partir de lo anterior, este Instituto advierte que a través de la de la PDN, l**os usuarios serán capaces de realizar consultas mediante el uso de APIs implementados por las Instituciones, dichas consultas se configurarán usando parámetros.** El API tendrá la tarea de recibir la consulta y aplicar la lógica de negocio al interior de la institución para generar la respuesta correspondiente.

En este sentido, l**a PDN logrará la interoperabilidad técnica con los diversos sistemas que la integrarán a través de la creación de estándares de datos y mediante el uso de Interfaces de Programación de Aplicaciones.** Los estándares de datos permitirán homologar la manera en que la información se debe representar para su entrega a la PDN, mientras que las APIs serán el mecanismo que permitirá la comunicación entre sistemas a través de Internet. Las APIs son ampliamente usadas para el desarrollo de aplicaciones a gran escala. El uso de APIs permitirá que las instituciones conserven el control de sus datos, gestionando el acceso a los mismos mediante reglas y perfiles de usuario.

Al respecto, se observa que la SESNA no recabará los datos personales que integrarán los sistemas que conforman la PDN, ya que dicha plataforma se conformará a partir de la información proporcionada por las autoridades que integran el SNA, a su vez proporcionada por los Entes públicos que en el marco de sus facultades se encuentran obligados a conformar la información de los sistemas S1, S2. S3 y S6.

De tal manera, que la PDN se integrara con las siguientes fuentes de información:

- **S1** se alimentará del Sistema de Evolución Patrimonial de Declaración de Intereses y Constancia de Prestación de Declaración Fiscal mejor conocido como DeclaraNet.
- **S2** se alimentará del Registro de Servidores Púbicos del Gobierno Federal conocido como RUSP, el Registro de Servidores Públicos de la Administración Pública Federal que intervienen en procedimientos de contrataciones públicas y de las Unidades Compradoras de CompraNet.
- **S3** se alimentará del Registro de Servidores Públicos Sancionados; Sistema de procedimientos administrativos de responsabilidades y el Sistema Integral de Responsabilidades Administrativas.
- **S6** se alimentará de CompraNet y la Bitácora Electrónica de Obra Pública.

Finalmente, es posible advertir tres posibles fases en el tratamiento de datos personales: la primera, la integración y conexión de los diversos sistemas; la segunda, la consulta a dicha información por parte de los diferentes perfiles de usuarios, y finalmente la tercera fase que corresponde a la consulta, disposición e intercambio de información que determinados usuarios tendrán de la misma. En esta fase, se encuentra incluida los datos personales de carácter confidencial del S1.

En este sentido, la SESNA tendrá la administración de la plataforma, de conformidad con lo establecido en el articulo 48 de la Ley General del Sistema Nacional, obtendrá y dará tratamiento, de manera indirecta, a datos los personales contenidos en los sistemas mencionados, para el cumplimiento de sus funciones que, en el caso que nos ocupa y de conformidad con lo dispuesto en el articulo 49 de la Ley General del Sistema Nacional se traducen en la conformación de la PDN.

Lo anterior, restringe o nulifica que la SESNA obtenga y trate los datos personales que darán contenido a la PDN a través de medios engañosos y fraudulentos, al estar definidas expresamente las fuentes a través de las cuales puede allegarse de datos personales, concretamente:

- **S1.** Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal.
- **S2.** Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas.
- **S3.** Sistema nacional de Servidores públicos y particulares sancionados.
- **S6.** Sistema de Información Pública de Contrataciones.

Ahora bien, con respecto al requerimiento que exige el principio de lealtad relacionado con respetar la expectativa razonable de privacidad del titular, conviene manifestar que las Bases para el funcionamiento de la PDN, disponen que para el funcionamiento de la plataforma, se tendrá en cuenta en todo momento las disposiciones en materia de protección de datos personales en posesión de los

sujetos obligados; que permitan cumplir con los procedimientos, obligaciones y disposiciones del Sistema Nacional Anticorrupción y las instituciones que lo conforman, así como que la Secretaría Ejecutiva establecerá los mecanismos de seguridad necesarios que garanticen la confidencialidad, integridad y disponibilidad de la información.

No obstante, no se advierte de manera expresa la existencia de previsiones normativas que prohíben a la SESNA tratar los datos personales que integrarán la PDN para finalidades distintas a aquéllas que justifican su obtención y que son indicadas en el aviso de privacidad correspondiente, en cumplimiento de las disposiciones previstas en la Ley General y los Lineamientos Generales.

Por lo cual, se sugiere a la SESNA establecer algún mecanismo que le permita acreditar su obligación de respetar la expectativa razonable de privacidad del titular, como podría ser de manera enunciativa más no limitativa, identificar requerimientos para la actualización o reforma de las Bases para el funcionamiento de la PND, o inclusive, determinar mecanismos de coordinación para el intercambio de información con las diversas partes interesadas.

En lo que respecta a la última condición a que se refieren los artículos 19 de la Ley General y 11, fracción II de los Lineamientos Generales, es decir, respetar la confianza que el titular ha depositado en el responsable respecto a que sus datos personales serán tratados conforme a lo señalado en el aviso de privacidad y en cumplimiento de las disposiciones previstas en la Ley General, los Lineamientos Generales y demás normatividad aplicable, de las manifestaciones de la SESNA y de las documentales presentadas no se advierte algún mecanismo concreto.

Por lo que se sugiere a la SESNA establecer algún mecanismo especifico que obligue a todos los usuarios de la PDN a privilegiar los intereses de los titulares, evitando que el tratamiento de los datos personales dé lugar a algún tipo de discriminación o trato injusto o arbitrario; por alguna vulneración en torno al deber de seguridad de la información, particularmente, sobre los atributos de integridad y disponibilidad de los datos personales.

Por lo cual, se concluye que no se cumple en su totalidad con el principio de lealtad a que se refieren los artículos 19 de la Ley General y 11, fracción I de los Lineamientos Generales en lo que respecta a la prohibición de obtener y tratar datos personales a través de medios engañosos o fraudulentos, así como respetar la expectativa razonable de privacidad del titular.

1.4 Principio de consentimiento

Los artículos 20, 21 y 22 de la Ley General, 12, 13, 14, 15, 16, 17, 18, 19 y 20 de los Lineamientos Generales de los cuales se desprende que el responsable está obligado a obtener el consentimiento

del titular, ya sea en su modalidad expresa o tácita, de manera previa al tratamiento de sus datos personales, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la Ley General:

- Cuando una ley así lo disponga debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en la Ley General, en ningún caso podrán contravenirla.
- Cuando se realicen transferencias de datos personales entre responsables para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
- Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.
- Para el reconocimiento o defensa de derechos del titular ante autoridad competente.
- Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
- Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o bienes.
- Cuando los datos personales sean necesarios para la prevención, diagnóstico, o la prestación de asistencia sanitaria.
- Cuando los datos personales figuren en fuentes de acceso público.
- Cuando los datos personales se sometan a un procedimiento previo de disociación.
- Cuando el titular sea una persona reportada como desaparecida en los términos de la ley en la materia.

Para tal efecto, el consentimiento del titular debe caracterizarse por ser:

- Libre: sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular.
- Específico: referido a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento de los datos personales.
- Informado: que el titular tenga conocimiento del aviso de privacidad previo al tratamiento de sus datos personales.

Por regla general, será válido el consentimiento tácito del titular para cualquier tratamiento de datos personales, salvo que una ley exija que la voluntad del titular se manifieste expresamente.

La solicitud del consentimiento debe ser concisa e inteligible, estar redactada en un lenguaje claro y sencillo acorde con el perfil del titular y, cuando se refiera a diversos asuntos ajenos a la protección

de datos personales, presentarse de tal forma que se distinga claramente de dichos asuntos. Lo anterior, en caso de que se requiera el consentimiento del titular para el tratamiento de sus datos personales.

Asimismo, el responsable está obligado a obtener el consentimiento del titular, de manera previa, cuando se recaben los datos personales directamente del titular y se requiera su consentimiento.

Cuando se recaben los datos personales indirectamente del titular y se requiera su consentimiento, el responsable tiene prohibido tratar los datos personales hasta que cuente con el consentimiento del titular.

Sobre el particular, la SESNA manifestó lo siguiente:

> *"[...]*
>
> *Al ser una plataforma de interoperabilidad, **la PDN no genera ni almacena los datos**, sino que a través de servicios web o API´s, consulta la información de los servidores y las bases de datos de los generadores de la información, y los refleja en la Plataforma.*
>
> ***La forma más fácil de entender el funcionamiento de la PDN es pensar en cualquier plataforma de internet para reservar vacaciones (Por ejemplo; Expedia). Con tan solo introducir fechas, lugar y rango de precios, la plataforma de reservaciones genera una búsqueda de opciones de vuelos y hoteles. Estas plataformas no generan los datos por sí mismas, se comunican con otros sistemas para permitir al usuario consultar de manera uniforme entre miles de opciones de diversos proveedores de información, con tan solo un clic.***
>
> ***La PDN opera con una arquitectura basada en comunicaciones a través de internet, que permite consultar información desde diversos proveedores de información (entes de gobierno), en tiempo real y de manera estandarizada (en un mismo formato). Con el objetivo de incorporar datos a la PDN, los generadores de información deben establecer mecanismos tecnológicos que permitan la consulta de información desde la PDN hacia sus bases de datos.***
>
> *[...]" (Sic)*

Aunado a lo anterior, en su Documento de seguridad, la SESNA manifestó lo siguiente:

> *"La obtención de la información y datos personales para este Sistema de tratamiento de datos personales es realizada por La Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos, según corresponda. Estas autoridades son los encargados de obtener la información y, por lo tanto, de obtener el consentimiento respectivo de los titulares ya que la Plataforma Digital Nacional es una plataforma de interoperabilidad que no genera ni almacena los datos."*

Como ya se mencionó, la SESNA no obtendrá directamente de los titulares, los datos personales que obran en cada uno de los cuatro sistemas que forman parte de la PDN ya que dicha plataforma se integrará a partir de la información de las bases de datos proporcionados por lo proveedores de información (Entes públicos) con atribuciones en la materia, a través de las autoridades integrantes del SNA para la conformación de la PDN, de conformidad con lo dispuesto en el artículo 49 de la Ley General del Sistema Nacional.

En otras palabras, la SESNA obtendrá los datos personales que obran en cada uno de los cuatro sistemas que forman parte de la PDN de manera indirecta del titular, es decir, a través de la comunicación entre sistemas de información que realizarán lo proveedores de información (Entes públicos) con atribuciones en la materia, por medio de las APIs como medio por el cual se da la interconexión de los diversos sistemas y se realizan dichas comunicaciones de datos personales entre ellos por medio de la PDN, permitiendo el acceso o consulta de los servidores y bases de datos de los generadores de la información conectados a la plataforma, actualizándose una transferencia, entendida como toda comunicación de datos personales, dentro o fuera de territorio mexicano, realizada a persona distinta del titular, responsable o encargado, de acuerdo con el artículo 3, fracción XXXII de la Ley General.

La PDN logrará la **interoperabilidad técnica** con los diversos sistemas que la integrarán a través de la creación de estándares de datos y mediante el uso de las APIs. Los estándares de datos permitirán homologar la manera en que la información se debe representar para su entrega a la PDN, mientras que las APIs serán el mecanismo que permitirá la comunicación entre sistemas a través de Internet. Las APIs son ampliamente usadas para el desarrollo de aplicaciones a gran escala. El uso de APIs permitirá que las instituciones conserven el control de sus datos, gestionando el acceso a los mismos mediante reglas y perfiles de usuario.

Para la incorporación de los datos a la PDN, los generadores de información deben establecer mecanismos tecnológicos que permitirán la consulta de información desde la PDN hacia sus bases de datos. En ese sentido, la SESNA es la responsable de publicar las Especificaciones Técnicas y Estándares de Datos[17] que permiten que cualquier ente público pueda desarrollar y poner en marcha los mencionados mecanismos de comunicación.

En este sentido, los responsables del tratamiento de datos personales, quienes recaban directamente de los titulares son los responsables del tratamiento de los sistemas:

1. **Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal (en adelante, S1),** que alimentará del Sistema de

Evolución Patrimonial de Declaración de Intereses y Constancia de Prestación de Declaración Fiscal mejor conocido como DeclaraNet.

2. **Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas (en lo sucesivo, S2), se** alimentará del Registro de Servidores Púbicos del Gobierno Federal, el Registro de Servidores Públicos de la Administración Pública Federal que intervienen en procedimientos de contrataciones públicas y de las Unidades Compradoras de CompraNet.
3. **Sistema nacional de Servidores públicos y particulares sancionados (en lo subsecuente, S3),** se alimentará del Registro de Servidores Públicos Sancionados; Sistema de procedimientos administrativos de responsabilidades y el Sistema Integral de Responsabilidades Administrativas.
4. Sistema de información y comunicación del Sistema Nacional y del Sistema Nacional de Fiscalización (en adelante, S4).
5. Sistema de denuncias públicas de faltas administrativas y hechos de corrupción (en lo sucesivo, S5).
6. **Sistema de Información Pública de Contrataciones (en lo subsecuente, S6), que** se alimentará de CompraNet y la Bitácora Electrónica de Obra Pública.

Al respecto, por lo que hace al tratamiento que **realizará la SESNA por medio de la PDN**, cabe recordar que el artículo 20 de la Ley General establece que será necesario recabar el consentimiento del titular para el tratamiento de sus datos personales, siempre y cuando no se actualice alguna de las causales de excepción previstas en el artículo 22 de la misma ley.

En este sentido, la fracción I del artículo 22 de la Ley General, establece que el responsable no estará obligado a recabar el consentimiento del titular cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en la Ley General.

Tomando en cuenta lo anterior, se observa que los sistemas que integran la PDN operan de manera independiente a la plataforma y su creación se encuentra establecida por la misma Ley General del Sistema Nacional, por lo que los responsables de dichos sistemas son quienes, en principio, se encuentran obligados a observar los principios y deberes establecidos en la normatividad aplicables entre los que se encuentra la obtención del consentimiento de los titulares para el tratamiento de datos personales que realicen, salvo que se actualice alguna causal de excepción.

Al respecto, por lo que hace al S1, la Ley General de Responsabilidades Administrativas, en sus artículos 32, 38, 39 y 46, establecen la obligación de todo servidor público a presentar su declaración patrimonial y de intereses, proporcionando la información requerida, incluyendo la de su cónyuge,

concubina o concubinario, dependientes económicos directos y terceros (socios comerciales, clientes, representantes y representados).

En virtud de lo anterior, no sería exigible el consentimiento del declarante, así como de los terceros referidos, ya que dicho tratamiento deriva del cumplimiento de las disposiciones contenidas en la Ley General de Responsabilidades, lo cual a su vez resulta compatible con su integración a la PDN, habilitada desde origen por los artículos 48 y 49 de la Ley General del Sistema Nacional en relación con el artículo 27 de la Ley General de Responsabilidades, en donde se señala que la información prevista en el sistema de evolución patrimonial, de declaración de intereses y de constancias de presentación de declaración fiscal se almacenará en la PDN que contendrá la información que para efectos de las funciones del Sistema Nacional Anticorrupción, generen los entes públicos facultados para la fiscalización y control de recursos públicos y la prevención, control, detección, sanción y disuasión de Faltas administrativas y hechos de corrupción, de conformidad con lo establecido en la Ley General del Sistema Nacional.

Ahora bien, por lo que hace al S2, el artículo 43 de la Ley General de Responsabilidades establece que la PDN incluirá, en un sistema específico, los nombres y adscripción de los servidores públicos que intervengan en procedimientos para contrataciones públicas, ya sea en la tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, el cual será actualizado quincenalmente.

Asimismo, por lo que hace al S3, el artículo 27 de la Ley General de Responsabilidades establece como obligación que en el sistema nacional de servidores públicos y particulares sancionados de la Plataforma digital nacional se inscribirán y se harán públicas, de conformidad con lo dispuesto en la Ley General del Sistema Nacional y las disposiciones legales en materia de transparencia, las constancias de sanciones o de inhabilitación que se encuentren firmes en contra de los Servidores Públicos o particulares que hayan sido sancionados por actos vinculados con faltas graves en términos de esta Ley, así como la anotación de aquellas abstenciones que hayan realizado las autoridades investigadoras o el Tribunal.

Finalmente, por lo que hace al S6, actualmente se encuentra previsto en la Ley de adquisiciones, arrendamientos y servicios del sector público, artículos 2, fracción II y 56, así como en los artículos 2 fracción II y 74 de la Ley de obras públicas y servicios relacionados con las mismas, establecen el sistema COMPRANET, señalando que la administración del sistema electrónico de información pública gubernamental sobre adquisiciones, arrendamientos y servicios, estará a cargo de la Secretaría de la Función Pública, a través de la unidad administrativa que determine su Reglamento,

en el cual las dependencias, entidades y los demás sujetos de la misma ley, deberán incorporar la información que esta les requiera.

Dicho sistema contendrá, por lo menos, la siguiente información, la cual deberá verificarse que se encuentra actualizada por lo menos cada tres meses:

a) Los programas anuales de adquisiciones, arrendamientos y servicios de las dependencias y entidades.
b) El registro único de proveedores.
c) El padrón de testigos sociales.
d) La información derivada de los procedimientos de contratación, en los términos de esta Ley.
e) Las notificaciones y avisos relativos a los procedimientos de contratación y de la instancia de inconformidades.
f) Los datos de los contratos suscritos, a que se refiere el artículo 7 fracción XIII, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
g) El registro de proveedores sancionados.
h) Las resoluciones de la instancia de inconformidad que hayan causado estado.

En este sentido, conforme a las disposiciones citadas, se advierte que dichos tratamientos se encuadran dentro de la fracción I del artículo 22 de la Ley General, en el entendido de que el responsable del tratamiento de los datos personales estará exceptuado de obtener el consentimiento cuando esté previsto en una ley.

Aunado a lo anterior, cabe señalar que, dentro del análisis respecto a la integración al S1 a la PDN, se refiere que la información ahí contenida podrá ser solicitada y utilizada por el Ministerio Público, los Tribunales o las autoridades judiciales en el ejercicio de sus respectivas atribuciones, el Servidor Público interesado o bien, cuando las Autoridades investigadoras, substanciadoras o resolutoras lo requieran con motivo de la investigación o la resolución de procedimientos de responsabilidades administrativas, esto de conformidad con lo establecido en el artículo 28 de la Ley General de Responsabilidades.

Caso en el cual se actualizarían transferencias de datos personales contenidos en el Sistema de evolución patrimonial, de declaración de interés y constancia de presentación de declaración fiscal, entendida como toda comunicación de datos personales, dentro o fuera de territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado, de conformidad con lo establecido en el artículo 3, fracción XXXII, de la Ley General, hacia las autoridades señaladas en principio, por el artículo 28 de la Ley General de Responsabilidades, al permitirse su consulta y acceso por medio de la PDN.

Al respecto, cabe señalar que por lo que hace al consentimiento, el artículo 65 de la Ley General, donde se contempla que toda transferencia de datos personales se encuentra sujeta al consentimiento del titular, salvo que se actualice alguna de las excepciones previstas en los artículos 22, 66 y 70 de la Ley General.

En tal virtud, para el caso concreto, cabe referir a lo establecido en la fracción I del artículo 70, que señala que el consentimiento no será necesario cuando la transferencia esté prevista en una ley, supuesto que se actualiza en el presente caso, tomando en consideración que la información contenida en el S1 podrá ser solicitada en principio, por las autoridades señaladas en el artículo 28 de la Ley General de Responsabilidades, de conformidad con sus facultades.

En este sentido, el Instituto determina que el tratamiento de datos personales que se lleva a cabo por parte de la SESNA para la implementación de la PDN, cumple con el principio de consentimiento a que se refieren los artículos 20 de la Ley General y 12 de los Lineamientos Generales, en el entendido de que el responsable está obligado a obtener el consentimiento del titular para el tratamiento de sus datos personales, siempre y cuando no se actualice alguna de las excepciones previstas en el artículo 22 de la Ley General.

Finalmente, cabe traer a colación lo estipulado en el artículo 65 de las Bases para el funcionamiento de la PDN, el cual establece que podrán incorporarse a la PDN, sistemas adicionales a los contemplados en el artículo 49 de la Ley General del Sistema Nacional, a propuesta de uno o más miembros del Comité Coordinador y previo dictamen técnico de la Secretaría Ejecutiva.

Al respecto, en caso de tratarse de sistemas cuyos datos sean generados o resguardados por autoridades que no formen parte del Comité Coordinador, se requerirá su consentimiento expreso para la inclusión mediante convenio que para tal efecto se celebre con la Secretaría Ejecutiva.

En este sentido, se recomienda a la SESNA que en los convenios a que se refiere el párrafo anterior, se reconozca expresamente que corresponderá a las autoridades correspondientes, recabar el consentimiento de los titulares según sea el caso, para el tratamiento de sus datos personales conforme a las atribuciones y funciones conferidas por ministerio de ley, en términos de los artículos 20 de la Ley General y 12 de los Lineamientos Generales o los que correspondan en las legislaciones estatales en la materia.

Lo anterior, siempre y cuando, de conformidad con la Ley General, los Lineamientos Generales y demás normatividad que resulta aplicable o con las legislaciones estatales en la materia y demás

ordenamientos derivados, el consentimiento de los titulares, según sea el caso, sea exigible al no actualizarse alguna causal de excepción.

1.5 Principio de calidad

Los artículos 23 y 24 de la Ley General establecen lo siguiente:

> *"**Artículo 23.** El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.*
> *Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.*
> *Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.*
> *Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.*
> ***Artículo 24.** El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en el artículo anterior de la presente Ley.*
> *En los procedimientos a que se refiere el párrafo anterior, el responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales."*
>
> *Los artículos 23 y 24 de la Ley General, 21 y 23 de los Lineamientos generales, de los cuales se desprende que el responsable tiene la obligación de adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que serán tratados, de tal manera que no se altere la veracidad de éstos y que correspondan con la realidad del titular.*

Asimismo, los artículos 21, 22 y 23 de los Lineamientos Generales prevén lo siguiente:

> *"Principio de Calidad*
> ***Artículo 21.** Para efectos del artículo 23 de la Ley General y los presentes Lineamientos generales, se entenderá que los datos personales son:*
> ***I.** Exactos y correctos: cuando los datos personales en posesión del responsable no presentan errores que pudieran afectar su veracidad;*
> ***II.** Completos: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable, y*
> ***III.** Actualizados: cuando los datos personales responden fielmente a la situación actual del titular.*

Presunción de calidad de los datos personales cuando se obtienen indirectamente del titular
Artículo 22. Cuando los datos personales fueron obtenidos indirectamente del titular, el responsable deberá adoptar medidas de cualquier naturaleza dirigidas a garantizar que éstos responden al principio de calidad, de acuerdo con la categoría de datos personales y las condiciones y medios del tratamiento.

Supresión de los datos personales
Artículo 23. *En la supresión de los datos personales a que se refiere el artículo 23. párrafo tercero de la Ley General, el responsable deberá establecer políticas, métodos y técnicas orientadas a la supresión definitiva de éstos, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.*
En el establecimiento de las políticas, métodos y técnicas a que se refiere el párrafo anterior, el responsable deberá considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales:
I. Irreversibilidad: *que el proceso utilizado no permita recuperar los datos personales;*
II. Seguridad y confidencialidad: *que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General y los presentes Lineamientos generales, y*
III. Favorable al medio ambiente: *que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente."*

De lo anterior se desprende que el responsable tiene la obligación de adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales que serán tratados, de tal manera que no se altere la veracidad de éstos y que correspondan con la realidad del titular.

Se entiende que los datos personales son:

- Exactos y correctos: cuando los datos personales en posesión del responsable no presentan errores que pudieran afectar su veracidad.
- Completos: cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable.
- Actualizados: cuando los datos personales responden fielmente a la situación actual del titular.

Se presume el cumplimento del principio de calidad cuando los datos personales sean obtenidos de manera directa del titular. De lo contrario, si los datos personales son obtenidos de manera indirecta, el responsable está obligado a adoptar medidas de cualquier naturaleza dirigidas a garantizar que éstos responden al principio de calidad, de acuerdo con la categoría de datos personales y las condiciones y medios del tratamiento.

Al respecto, la SESNA manifestó en la presentación de la evaluación de impacto respecto de la PDN, lo siguiente:

"[...]

*Al ser una plataforma de interoperabilidad, **la PDN no genera ni almacena los datos**, sino que a través de servicios web o API's8, consulta la información de los servidores y las bases de datos de los generadores de la información, y los refleja en la Plataforma.*

En otras palabras, la PDN opera con una arquitectura basada en comunicaciones a través de Internet, que permite consultar información desde diversos proveedores de información (Entes públicos), en tiempo real y de manera estandarizada (en un mismo formato).
[...]
Vulnerabilidades
Es fundamental destacar que la PDN es una plataforma de interoperabilidad y, como lo establece la normatividad vigente (Bases de la PDN, LGRA, LGSNA), los Encargados son los responsables de recabar, ordenar y/o resguardar los datos e información en los subsistemas para su conexión con los sistemas de la PDN.
[...]

2. ***Información inexacta y/o equivocada**: Cuando los Encargados transfieren a la PDN información inexacta, campos adicionales, datos reservados y otro tipo de información que por sus características no debe ser pública o parte de la PDN.*
[....]
Protocolo de actuación
[...]

3. ***Información inexacta y/o equivocada:** Los Encargados deberán en todo momento revisar y asegurarse de que los datos interoperables con la PDN corresponden exclusivamente con la legislación vigente para cada uno de sus sistemas.*

En caso de que los datos personales contenidos en los expedientes sean inexactos o requieran actualizarse, se deberá realizar el procedimiento correspondiente con el Encargado, es decir la autoridad, ente o institución encargada de obtener y registrar la información en las bases de datos. Como lo establecen las Bases para el funcionamiento de la PDN, la información, su actualización y publicación es exclusivamente responsabilidad de los Encargados.
[...]
VII. CICLO DE VIDA DE LOS DATOS PERSONALES
La PDN no recaba, almacena, ni genera los datos consultables en cada sistema. Por lo tanto, no tiene acceso a las bases de datos ni tiene facultades para capturar, modificar o eliminar los datos contenidos en cada sistema. A través de la Plataforma se podrán consultar datos contenidos en diversas bases de datos, en tiempo real y de forma estandarizada.

Los plazos de conservación o almacenamiento de los datos personales y las técnicas para el borrado seguro de los datos será responsabilidad de las instituciones, dependencias u organismos que recaban la información y dueños de las bases de datos.

[...]" (Sic)

Aunado a lo anterior, en el documento denominado "Documento de seguridad", anexo de la evaluación de impacto en la protección de datos personales presentada por la SESNA, se advierte lo siguiente:

S1

"La obtención de la información y datos personales para este Sistema de tratamiento de datos personales es realizada por La Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos, según corresponda.

[...]

El uso, manejo y aprovechamiento de la información contenida en este Sistema tiene como objeto permitir la consulta de los datos de los servidores públicos obligados a presentar declaración patrimonial y de intereses, así como de garantizar la inscripción de la constancia de la declaración anual de impuestos que emita la autoridad fiscal competente.

[...]

El almacenamiento de la información y datos personales se realiza en los sistemas informáticos que poseen los Encargados de recabar la información en los distintos niveles de gobierno y órganos autónomos. Se reitera que, al ser la PDN, una plataforma que permite la interoperabilidad de distintos sistemas informáticos, no se realiza el almacenamiento, resguardo o replicación de la información contenida en las bases de datos de las autoridades responsables de recabarla.

El bloqueo de la información y datos personales es responsabilidad de los Encargados, es decir, las autoridades encargadas de recabar la información, ya que son éstas las que tendrán acceso a la información almacenada en sus bases de datos.

La información y datos personales será resguardada por las autoridades encargadas de su obtención, de acuerdo con la normatividad aplicable.

En cuanto a la supresión de la información y datos personales, nuevamente se enfatiza que estos procesos serán responsabilidad de las autoridades responsables y encargadas de las bases de datos o sistemas que recaban la información. La SESNA, como administrador de la PDN, no tiene la capacidad o atribuciones para alterar las bases de datos originales.

[...]

La obtención de la información y datos personales en este sistema lo deben realizar las autoridades que realicen procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos.

El uso, manejo y aprovechamiento de la información y datos personales en este sistema tiene como objeto permitir que el público en general tenga acceso a la información relacionada con los servidores públicos que intervienen en procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, de tal manera que sea utilizada por los integrantes del Sistema Nacional Anticorrupción y autoridades competentes en la prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.

El almacenamiento, bloqueo, resguardo o supresión de la información y datos personales es responsabilidad de los Encargados. Esto significa, las autoridades a las que pertenecen las personas servidoras públicas que intervienen en procedimientos de contrataciones públicas. Se reitera que la PDN es únicamente una plataforma de interoperabilidad por lo que no tiene facultades ni capacidades para alterar o administrar las bases de datos de los sistemas que contienen la información y datos personales.
[...]
La obtención de la información y datos personales en este sistema lo deben realizar las autoridades que realicen procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos.

El uso, manejo y aprovechamiento de la información y datos personales en este sistema tiene como objeto permitir que el público en general tenga acceso a la información relacionada con los servidores públicos que intervienen en procedimientos de contrataciones públicas, de tramitación, atención y resolución para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como en la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos, de tal manera que sea utilizada por los integrantes del Sistema Nacional Anticorrupción y autoridades competentes en la prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.
[...]
El almacenamiento, bloqueo, resguardo o supresión de la información y datos personales es responsabilidad de los Encargados. Esto significa, las autoridades a las que pertenecen las personas servidoras públicas que intervienen en procedimientos de contrataciones públicas. Se reitera que la PDN es únicamente una plataforma de consulta e interoperabilidad por lo que no tiene facultades ni capacidades para alterar o administrar las bases de datos de los sistemas que contienen la información y datos personales." (Sic)

Una vez precisado lo anterior, debe reiterarse que la PDN, al ser una plataforma de interoperabilidad no recaba, genera ni almacena los datos personales que conformarán la PDN, ya que dicha plataforma se conformará a partir de la información proporcionada por las autoridades que integran el SNA, a su vez proporcionada por los entes públicos que en el marco de sus facultades se encuentran obligados a conformar la información de los sistemas S1, S2, S3 y S6.

De esta manera, se aprecia que la obtención directa de los datos personales que forman parte de la información que integra los diferentes sistemas de la PDN la realizan los entes públicos en el marco de sus atribuciones, en su calidad de proveedores de proporcionar los datos e información, en tiempo y forma, de conformidad con la legislación aplicable.

Asimismo, y de conformidad con lo establecido en las Bases para el funcionamiento de la PDN, será obligación de los proveedores, a través de sus encargados y concentradores, vigilar la homologación, actualización y disponibilidad de la información que sea transferida de los subsistemas y conjuntos de datos a los sistemas de la PDN, de conformidad con la normativa aplicable, y verificar de manera permanente el correcto funcionamiento de los subsistemas y conjuntos de datos, así como sus

procesos de generación, estandarización, actualización y distribución de información a los sistemas, de acuerdo con las disposiciones emitidas por la Secretaría Ejecutiva, para asegurar el correcto funcionamiento de la Plataforma.

Aunado a lo anterior, y de conformidad con lo manifestado por la SESNA, los encargados, como parte de los proveedores de la información que conformará la PDN, deberán en todo momento revisar y asegurarse de que los datos interoperables con la PDN corresponden exclusivamente con la legislación vigente para cada uno de sus sistemas y no así comunicar a la PDN información inexacta y/o equivocada, tales como campos adicionales, datos reservados y otro tipo de información que por sus características no debe ser pública o parte de la PDN.

En caso de que los datos personales contenidos en los expedientes sean inexactos o requieran actualizarse, se deberá realizar el procedimiento correspondiente con el encargado, es decir la autoridad, ente o institución encargada de obtener y registrar la información en las bases de datos. Como lo establecen las Bases para el funcionamiento de la PDN, la información, su actualización y publicación es exclusivamente responsabilidad de los encargados.

No obstante lo anterior, la SESNA tendrá la administración de la plataforma, de conformidad con lo establecido en el artículo 48 de la Ley General del Sistema Nacional, además de que obtendrá y dará tratamiento, de manera indirecta, a los datos personales contenidos en los sistemas mencionados, para el cumplimiento de sus funciones que, en el caso que nos ocupa y de conformidad con lo dispuesto en el artículo 49 de la Ley General del Sistema Nacional se traducen en la conformación de la PDN por lo cual, para la presunción del cumplimiento del principio de calidad de los datos personales, la SESNA deberá adoptar medidas de cualquier naturaleza dirigidas a garantizar que éstos responden al principio de calidad, de acuerdo con la categoría de datos personales y las condiciones y medios del tratamiento, de conformidad con lo dispuesto en el artículo 22 de los Lineamientos Generales.

De esta manera y derivado de las facultades y atribuciones asignadas a la SESNA, ésta tiene la obligación de emitir los protocolos, estándares, reglamentos, especificaciones técnicas y cualquier normativa necesaria para la colaboración, provisión de datos y acciones para cumplir con las Bases, los cuales serán obligatorios para todos los proveedores, concentradores y encargados a nivel federal, estatal y municipal.

En este sentido, y de conformidad con la información expuesta en la página web de la PDN, se puede advertir que la SESNA tiene publicadas las especificaciones técnicas que refieren a las reglas y

características con las que deben de contar los datos para la interoperabilidad de los sistemas 1, 2 y 3 en la página oficial de la PDN para consulta pública[17].

Al respecto, cabe señalar que estas especificaciones refieren a los campos mínimos de datos que debe de contener cada sistema a través de un diccionario de datos que determina la SESNA; así como los estándares que debe de seguir cada campo para ser interoperable con la PDN y su vez puedan ser consultados en la plataforma. Es decir, los estándares de datos permitirán homologar la manera en que la información se debe representar para su entrega a la PDN.

Respecto de los estándares, es preciso indicar que la SESNA también cuenta con una herramienta denominada "Versionado del Estándar de Datos" para la interoperabilidad del Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal (S1), en el cual se determina un calendario en el que se prevén modificaciones a los estándares de datos, así como los supuestos por los cuales se realiza esta modificación efecto de garantizar la homologación de la información de todas las autoridades que proporcionen información a la PDN.

De igual forma refiere, al formato de especificación que permite describir de manera precisa las características con las cue deberán contar las APIs que integrarán a la PDN, entendiendo que las APIs se constituyen como el mecanismo que permitirá la comunicación entre sistemas a través de Internet.

De manera adicional, la SESNA cuenta con un mecanismo de pruebas para la interconexión de los sistemas con la PDN y con ello verificar el funcionamiento de las APIs. Así como con un "Validador de datos" el cual ayudará a las autoridades a verificar que la respuesta generada por sus APIs cumple las especificaciones que se refieren a los campos mínimos de datos que debe contener cada sistema, así como el estándar que debe seguir cada campo para ser interoperable con la PDN.

De esta manera, la SESNA otorga el modelo de interoperabilidad que deberán adoptar los diversos sistemas de que proveerán información a la PDN.

De las consideraciones anteriores, es posible advertir que los datos personales tratados por la SESNA serán exactos y correctos toda vez que, con la herramienta para validar los datos, se busca que, a través de la comparación de la información que los proveedores proporcionen con los estándares y campos mínimos de datos personales que debe tener cada sistema de la PDN, estos no presenten errores que pudiera afectar su veracidad.

[17] Disponible en el siguiente vínculo electrónico: https://www.plataformadetransparencia.org.mx/especificaciones, consultado por última vez el 18/05/2021.

Asimismo, se advierte que, a través de los formatos establecidos para las APIs y los mecanismos de prueba, los datos personales tratados por la SESNA serán completos toda vez que al verificar el funcionamiento y conexión de las APIs como medios del tratamiento permitirán su integridad y por ende el cumplimiento de las finalidades que motivaron su tratamiento como lo es la interoperabilidad, acceso y consulta.

No obstante, este Instituto no pudo advertir si los datos personales tratados a través de la PDN, serán actualizados pues no se desprende información que permita acreditar que se tienen establecidos controles para garantizar que estos respondan fielmente a la situación actual del titular, por lo que se advierte un cumplimiento parcial de la calidad de los datos personales que conforman los diversos sistemas de la PDN, por lo cual este Instituto recomienda a la SESNA, establecer mecanismos, procesos y controles administrativos y técnicos para garantizar la calidad los datos personales que permitan que los datos personales sean actualizados en función de la naturaleza de la información respecto de los sistemas 1, 2 y 3, y contemplar el establecimiento de dichos mecanismos, procesos y controles administrativos y técnicos para garantizar la calidad los datos personales en el tratamiento de los sistemas 4, 5 y 6.

Asimismo, con independencia de que sean los encargados los responsables de alimentar las bases que conforman los sistemas de la PDN, y en este sentido sean quienes en primera instancia cumplan con el principio de calidad, la SESNA como administradora de la plataforma debe asegurarse que la configuración de la interoperabilidad y los accesos a las bases de datos de los distintos sistemas por medio de las APIs, garantice que dicha consulta se efectúe respecto a las bases en su última versión, es decir aquella con la información más actualizada.

Por otro lado, el principio de calidad también implica que el responsable está obligado a suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, previo bloqueo en su caso y una vez que concluya el periodo de conservación de los datos personales.

Es por ello, que el responsable tiene la obligación de:

- Establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que serán utilizados. En la definición de los plazos de conservación de los datos personales se deberán considerar los valores administrativos, contables, fiscales, jurídicos e históricos que pudieran llegar a tener éstos.

- Establecer políticas, métodos y técnicas orientadas a la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima. Para ello deberá considerar los siguientes factores:
  - Irreversibilidad: que el proceso utilizado no permita recuperar los datos personales.
  - Seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad.
  - Favorable al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.

Al respecto, la SESNA manifestó en la evaluación de impacto presentada, lo siguiente:

"[…]

CICLO DE VIDA DE LOS DATOS PERSONALES
La PDN no recaba, almacena, ni genera los datos consultables en cada sistema. Por lo tanto, no tiene acceso a las bases de datos ni tiene facultades para capturar, modificar o eliminar los datos contenidos en cada sistema. A través de la Plataforma se podrán consultar datos contenidos en diversas bases de datos, en tiempo real y de forma estandarizada.

Los plazos de conservación o almacenamiento de los datos personales y las técnicas para el borrado seguro de los datos será responsabilidad de las instituciones, dependencias u organismos que recaban la información y dueños de las bases de datos.
[…]" (Sic)

Aunado a lo anterior, en el documento denominado "Documento de seguridad", anexo de la evaluación de impacto en la protección de datos personales presentada por la SESNA, se advierte lo siguiente:

S1
"[…]
El almacenamiento de la información y datos personales se realiza en los sistemas informáticos que poseen los Encargados de recabar la información en los distintos niveles de gobierno y órganos autónomos. Se reitera que, al ser la PDN, una plataforma que permite la interoperabilidad de distintos sistemas informáticos, no se realiza el almacenamiento, resguardo o replicación de la información contenida en las bases de datos de las autoridades responsables de recabarla.

El bloqueo de la información y datos personales es responsabilidad de los Encargados, es decir, las autoridades encargadas de recabar la información, ya que son éstas las que tendrán acceso a la información almacenada en sus bases de datos.

La información y datos personales será resguardada por las autoridades encargadas de su obtención, de acuerdo con la normatividad aplicable.

En cuanto a la supresión de la información y datos personales, nuevamente se enfatiza que estos procesos serán responsabilidad de las autoridades responsables y encargadas de las bases de datos o sistemas que recaban la información. La SESNA, como administrador de la PDN, no tiene la capacidad o atribuciones para alterar las bases de datos originales.
[...]"

S2
"[...]
El almacenamiento, bloqueo, resguardo o supresión de la información y datos personales es responsabilidad de los Encargados. Esto significa, las autoridades a las que pertenecen las personas servidoras públicas que intervienen en procedimientos de contrataciones públicas. Se reitera que la PDN es únicamente una plataforma de interoperabilidad por lo que no tiene facultades ni capacidades para alterar o administrar las bases de datos de los sistemas que contienen la información y datos personales."

S3
[...]
El almacenamiento, bloqueo, resguardo o supresión de la información y datos personales es responsabilidad de los Encargados. Esto significa, las autoridades a las que pertenecen las personas servidoras públicas que intervienen en procedimientos de contrataciones públicas. Se reitera que la PDN es únicamente una plataforma de consulta e interoperabilidad por lo que no tiene facultades ni capacidades para alterar o administrar las bases de datos de los sistemas que contienen la información y datos personales." (Sic).

Por otro lado, en el requerimiento de Información adicional, la SESNA señaló:

"La información se consulta desde las bases de datos de los entes públicos interconectados con la PDN a través de APIs REST, residiendo temporalmente en memoria volátil. Al no existir almacenamiento persistente, no se requiere efectuar borrados seguros periódicamente." (Sic).

Ahora bien, específicamente, sobre el mecanismo de borrado seguro la Ley General menciona lo siguiente:

"Artículo 23.
[...]
Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos."

Por su parte, los Lineamientos Generales indican que:

*"**Supresión de los datos personales***
***Artículo 23.** En la supresión de los datos personales a que se refiere el artículo 23, párrafo tercero de la Ley General, el responsable deberá establecer políticas, métodos y técnicas orientadas a la*

> *supresión definitiva de éstos, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.*
>
> *En el establecimiento de las políticas, métodos y técnicas a que se refiere el párrafo anterior, el responsable deberá considerar, al menos, los siguientes atributos y el o los medios de almacenamiento, físicos y/o electrónicos en los que se encuentren los datos personales:*
>
> *I. **Irreversibilidad:** que el proceso utilizado no permita recuperar los datos personales;*
> *II. **Seguridad y confidencialidad:** que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General y los presentes Lineamientos generales, y*
> *III. **Favorable al medio ambiente**: que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente." (Sic).*

Al respecto, el responsable (SESNA) menciona que al ser una plataforma de interoperabilidad no almacena datos personales, aunque, almacena datos incluidos por la navegación y uso de la plataforma, información que se comentó se autodestruía y solo se utilizaban datos anonimizados para fines estadísticos, lo cual no está indicado en algún documento que ponga en evidencia la implementación de un método o técnica para el borrado de los datos de navegación dentro de la plataforma.

De la, lectura del documento, se asume que la información recibida por la PDN no tiene persistencia en esta plataforma, sin embargo, si bien es cierto que no se almacena a propósito, esta si puede ser almacenada por los elementos que conforman la arquitectura de la PDN para otros propósitos, por ejemplo: de cache. El no describir la tecnología utilizada en la PDN dificulta contar con elementos para cerciorarse que lo asumido es cierto y que no hay posibilidad de que haya remanentes de información en los componentes de la arquitectura de la plataforma.

Visto lo anterior, este Instituto determina que la SESNA no presentó la documentación que acredite las técnicas a utilizar para garantizar el borrado seguro de los datos personales, en atención a la obligación establecida en el artículo 23, de la Ley General y 23 de los Lineamientos generales, es decir, no contempló métodos y/o técnicas para garantizar el borrado de los datos de navegación al no incluir evidencias que den soporte a las manifestaciones realizadas sobre un proceso de anonimización de los datos utilizados para fines estadísticos.

1.6 Principio de proporcionalidad

El artículo 25 de la Ley General establece lo siguiente:

> *"**Artículo 25.** El responsable sólo deberé tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento." (Sic).*

A su vez, los artículos 24 y 25 de los Lineamientos generales señalan lo siguiente:

> *"**Principio de proporcionalidad***
> ***Artículo 24.** En términos del artículo 25 de la Ley General y los presentes Lineamientos generales, se entenderá que los datos personales son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas al responsable por la normatividad que le resulte aplicable.*
>
> ***Criterio de minimización***
> ***Artículo 25.** El responsable deberá realizar esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, con relación a las finalidades que motivan su tratamiento." (Sic).*

De las disposiciones citadas, se observa que el responsable está obligado a recabar y utilizar los datos personales que resulten estrictamente necesarios y pertinentes para los objetivos que persigue, de acuerdo con las atribuciones conferidas al responsable por la normatividad que le resulte aplicable, así como realizar esfuerzos razonables para limitar los datos personales tratados al mínimo necesario, con relación a las finalidades que motivan su tratamiento.

Ahora bien, el análisis del principio de proporcionalidad, en el caso concreto, debe dirigirse a determinar si los datos personales de la información que conforman los diferentes sistemas integrantes de la PDN son adecuados, pertinentes y no excesivos para el cumplimiento de las finalidades que conlleva la puesta en operación de esta plataforma.

Ahora bien, el tratamiento de datos personales que se llevará a cabo a través de la PDN se realiza en atención a las atribuciones y funciones que le han sido conferidas a la SESNA como administradora de dicha plataforma y conforme a las finalidades que ha señalado como finalidades específicas, a saber:

- La interoperabilidad, interconexión, estabilidad, uso y seguridad de la información integrada en la Plataforma, esto es, contar con una plataforma que integre y conecte los diversos sistemas electrónicos que posean datos e información necesaria para que las autoridades competentes tengan acceso a los 6 sistemas a que se refiere el Título Cuarto de la Ley General del Sistema Nacional:
    - Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal;
    - Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas;
    - Sistema nacional de Servidores públicos y particulares sancionados;

  - Sistema de información y comunicación del Sistema Nacional y del Sistema Nacional de Fiscalización;
  - Sistema de denuncias públicas de faltas administrativas y hechos de corrupción, y
  - Sistema de Información Pública de Contrataciones.
- Promover la homologación de procesos, estandarización de datos y la simplicidad del uso para los usuarios;
- Tener en cuenta en todo momento los derechos de acceso a la información y protección de datos personales en posesión de los sujetos obligados; que permitan cumplir con los procedimientos, obligaciones y disposiciones del Sistema Nacional Anticorrupción y las instituciones que lo conforman.
- Que los diferentes usuarios de la PDN puedan consultar la información dentro de cada uno de los sistemas de información, para las diferentes funcionalidades y alcances de acuerdo con cada perfil, a través de la conexión con diferentes fuentes de origen a saber:

  - Con un ecosistema federal que incluya el conjunto de datos que generarán las entidades públicas a nivel federal, es decir, los Poderes Ejecutivo, Legislativo y Judicial, por los Órganos Constitucionalmente Autónomos, así como por las Empresas Productivas del Estado, y por cualquier otra entidad con naturaleza diferente a éstas que opere a nivel federal.
  - Simultáneamente cada uno de los sistemas de la PDN deberá conectarse con los conjuntos de datos que hay en cada una de las 32 Entidades Federativas. Se deberá contemplar que cada Sistema Local Anticorrupción deberá contar con ese espejo de la PDN que contenga la información que se genera en cada Entidad Federativa, y que, a través de cada Secretaría Ejecutiva de los Sistemas Locales, se concentrará y conectará la información con la PDN.
- Contar con una fuente de **inteligencia para construir integridad y combatir la corrupción,** que creará valor para el gobierno y la sociedad, a partir de grandes cantidades de datos.
- Un **medio para el intercambio de datos anticorrupción**, que busca quitar barreras y romper silos de información para que los datos sean comparables, accesibles y utilizables, empezando con **seis sistemas de datos prioritarios, interoperables, estandarizados y distribuidos para ser consultados desde la Plataforma**.
- Permitir **el intercambio y consulta de datos eficiente** con autoridades y ciudadanía, cuidando en todo momento la seguridad e integridad de la información.

Asimismo, mediante el uso de **nuevas tecnologías, metodologías de trabajo, ciencia de datos e inteligencia artificial** como insumos y apoyo al trabajo de las autoridades del **SNA** para:

- **Analizar, predecir y alertar** a las autoridades sobre posibles riesgos de corrupción.

- **Automatizar procesos, evitar discrecionalidad, colusión y conflicto de interés.**
- **Promover el uso de los datos** para respaldar sanciones y como evidencia para combatir la impunidad.
- **Dar seguimiento, en tiempo real**, a los procesos y proyectos de contratación pública, asegurar el cumplimiento de sus objetivos y garantizar una mayor eficiencia en las compras públicas.
- **Apoyar la participación ciudadana**, poniendo al ciudadano al centro del combate a la corrupción.
- **Incorporar información sobre indicadores** para evaluar la Política Nacional Anticorrupción y el fenómeno en México.
- **Dar evidencia para generar recomendaciones de política pública** a las autoridades del Sistema Nacional Anticorrupción.

Asimismo, cabe señalar que la PDN **asegurará la interoperabilidad de la información que se conecte e integre, así como la que se genere, en cada sistema y entre los diversos sistemas.** Además, deberá contemplar la exportación de información por parte de los usuarios, de conformidad con el acceso determinado en el catálogo de perfiles que el uso de la información será responsabilidad de cada usuario, de conformidad con la normativa aplicable.

Al respecto, cabe señalar que cada uno de los sistemas que la conforman, mismos que se refieren como objeto de la presente evaluación de impacto, esto es los sistemas S1, S2, S3 y S6 a su vez, tienen finalidades específicas, a saber:

S1. OBJETO DEL SISTEMA DE EVOLUCIÓN PATRIMONIAL, DE DECLARACIÓN DE INTERESES Y CONSTANCIA DE PRESENTACIÓN DE DECLARACIÓN FISCAL:

- Que la información del sistema pueda ser solicitada y utilizada de acuerdo con las necesidades de las diversas autoridades competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción, entre las que se encuentran el Ministerio Público, Tribunales o autoridades judiciales, servidores públicos, autoridades investigadoras, sustanciadores o resolutoras, entre otras;
- Dar acceso a la **información pública** de las declaraciones de situación patrimonial y de intereses a todos los ciudadanos;
- Permitir que la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los OICs de los Entes públicos realicen la verificación aleatoria de las declaraciones patrimonial, de intereses, y para identificar la evolución del patrimonio de los servidores públicos, y

- Permitir la expedición de certificaciones de la inexistencia de anomalías de las declaraciones presentadas por los servidores públicos, las cuales deberán anotarse en el sistema.

Ahora bien, para la consecución de las finalidades citadas, la SESNA requerirá llevar a cabo el tratamiento de datos personales, de los siguientes titulares, conforme lo siguiente:

Datos del declarante:

- Nombre.
- Primer y segundo apellido.
- Clave Única de Registro de Población (CURP).
- Registro Federal de Contribuyentes (RFC) y homoclave.
- Correo electrónico institucional.
- Correo electrónico personal/alterno.
- Número telefónico de casa.
- Número celular personal.
- Régimen matrimonial.
- Estado Civil.
- País de nacimiento.
- Fecha de nacimiento.
- Nacionalidad.
- Firma.
- Domicilio.
- Escolaridad (último grado de estudios).
- Institución educativa donde se realizaron los estudios.
- Lugar donde se ubica la institución educativa.
- Carrera o área de conocimiento.
- Estatus.
- Fecha de obtención del documento.
- Documento obtenido.
- Empleo/cargo/comisión.
- Nivel del empleo cargo o comisión.
- Función o actividad principal que desempeña en su empleo, cargo o comisión.
- Fecha de toma de posesión/conclusión del empleo, cargo o comisión.
- Nombre del ente público al cual se encuentra adscrita la plaza.
- Área de adscripción.
- Ámbito público.

- Nivel/orden de gobierno.
- Teléfono de oficina y extensión.
- Domicilio del empleo, cargo o comisión.
- Experiencia laboral.
- Años laborados.
- Ámbito/sector en el que se laboró.
- Ingresos netos del declarante.
- Bienes inmuebles.
- Vehículos.
- Bienes muebles.
- Inversiones.
- Cuentas bancarias.
- Otro tipo de valores/activos.
- Adeudos/pasivos.
- Préstamo o comodato por terceros.
- Participación en empresas, sociedades, asociaciones.
- Apoyos o beneficios públicos.
- Beneficios privados.
- Fideicomisos.
- Representación.

Datos del cónyuge del declarante:

- Nombre.
- Primer y segundo apellidos.
- CURP.
- RFC y homoclave.
- Relación con el Declarante.
- Estado civil.
- Lugar de nacimiento.
- Fecha de nacimiento.
- Nacionalidad.
- Lugar de residencia.
- Domicilio.
- Actividad laboral.
- Lugar de trabajo.
- Ingresos netos.

- Otros ingresos.
- Bienes inmuebles.
- Vehículos.
- Bienes muebles.
- Inversiones, cuentas bancarias u otro tipo de valores /activos.
- Adeudos/pasivos.
- Préstamo o comodato por terceros.
- Participación en empresas, sociedades, asociaciones.
- Apoyos o beneficios públicos.
- Beneficiarios privados.
- Fideicomisos.
- Representación.

Datos de los dependientes económicos del declarante:

- Nombre completo.
- Primer y segundo apellidos.
- CURP.
- RFC y homoclave.
- Parentesco con el declarante.
- Lugar de nacimiento.
- Fecha de nacimiento.
- Nacionalidad.
- Lugar de residencia.
- Domicilio.
- Actividad laboral.
- Lugar de trabajo.
- Ingresos netos.
- Otros ingresos.
- Bienes inmuebles.
- Vehículos.
- Bienes muebles.
- Inversiones, cuentas bancarias u otro tipo de valores /activos.
- Adeudos/pasivos.
- Préstamo o comodato por terceros.
- Participación en empresas, sociedades, asociaciones.
- Apoyos o beneficios públicos.

- Beneficiarios privados.
- Fideicomisos.
- Representación.

Datos de los clientes principales del servidor público/pareja/dependiente económico:

- Nombre completo.
- RFC.
- Sector productivo al que pertenece.
- Servicio que proporciona.
- Lugar donde se ubica.

Datos de terceros relacionados con el declarante:

- Nombre completo.
- RFC.
- Dato que permita su identificación.
- Relación del transmisor del vehículo con el titular.
- Relación del transmisor de la propiedad con el titular.
- Relación con el dueño o titular.

Datos de servidores públicos que intervienen en procedimientos de contrataciones públicas:

- Nombre completo del servidor público.
- Nombre completo de la persona servidora pública que funge como superior jerárquico.
- RFC del servidor público.
- CURP del servidor público.
- RFC de la persona servidora pública que funge como superior jerárquico.
- CURP persona servidora pública que funge como superior jerárquico.

Datos de particulares, personas físicas y morales, que se encuentren inhabilitados para celebrar contratos con entes públicos:

- Nombre.
- RFC.
- Tipo de falta.
- Causas, motivos o hechos de sanción.

Datos personales de servidor público sancionado:

- Nombre del servidor público sancionado.

- Género servidor público sancionado.
- RFC servidor público sancionado.
- CURP servidor público sancionado.
- Dependencia.
- Tipo de falta.
- Causas, motivos o hechos de la sanción.
- Tipo de sanción.

Datos personales de particulares sancionados:

- Nombre del particular sancionado.
- RFC del particular sancionado.
- Dependencia.
- Tipo de falta.
- Causas, motivos o hechos de la sanción.
- Tipo de sanción.

Datos personales de servidores públicos y particulares que intervienen y participan en los procedimientos de contrataciones públicas, y personas físicas a las que se les adjudica un contrato público:

- Nombre de las personas servidoras públicas que intervienen en los procedimientos de contrataciones públicas.
- Nombre de las personas físicas que participan en procedimientos de contrataciones públicas.
- Nombre de las personas físicas a las que se las adjudica un contrato público.

En este sentido, la motivación respecto de los datos personales que serán requeridos para el propio funcionamiento de la PDN, así como para permitir la realización de consultas a los sistemas que conforman la plataforma por parte de los diferentes usuarios, encuentran sustento y justificación en los artículos 113 de la Constitución Política, 8, 9, fracción IX, 48, 49, 50, 51, 52, 53, 54, 55 y 56 de la Ley General del Sistema Nacional; así como en las Bases para el funcionamiento de la PDN, siendo éstos proporcionales o idóneos que permita a la SESNA el cumplimiento de las finalidades ya multicitadas.

Por lo tanto, del análisis de los datos personales con relación a las finalidades generales de la propia PDN, así como de las finalidades específicas respecto de los sistemas que la conforman que motivan el tratamiento de éstos por parte de la SESNA, se concluye que resultan adecuados, pertinentes y no excesivos para el cumplimiento de las atribuciones que le han sido encomendadas a la SESNA a través de la normatividad aplicable.

Al respecto, se observa que las finalidades antes señaladas encuentran aún mayor justificación al considerar la justificación de la SESNA sobre la necesidad de implementar la PDN:

> *"Su puesta en operación es estrictamente necesaria ya que corresponde a una obligación legal y generará grandes beneficios en el combate a la corrupción y la rendición de cuentas. Permitirá una mayor transparencia en el uso de recursos públicos y la actuación de los servidores públicos de todos los niveles de gobierno."*

Conforme a lo anterior, aunado al análisis de las finalidades y los objetivos concretos de la PDN, podría considerarse que el papel que ocupa la Plataforma dentro del SNA y el combate a la corrupción en México, es ser fuente de información fidedigna, herramienta indispensable para el seguimiento de procedimientos contemplados en la normatividad aplicable y mecanismo de rendición de cuentas en el combate a la corrupción.

En este sentido, la puesta en operación de la PDN cumple con el principio de proporcionalidad a que se refieren los artículos 25 de la Ley General y 24 y 25 de los Lineamientos generales, en el entendido que los datos antes enlistados anteriormente y que serán parte de la información que conformarán los sistemas que integran la PDN serán los estrictamente necesarios para el cumplimiento de las finalidades ya señaladas, considerando como fin ulterior el combate a la corrupción como una política del Estado mexicano y la necesidad de mecanismos, como la PDN, para la rendición de cuentas en el combate a la corrupción.

1.7 Principio de información

Los artículos 3, fracción II, 26, 27 y 28 de la Ley General, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43 y 44 de los Lineamientos generales, de los cuales se advierte que el responsable está obligado a informar al titular sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a través del aviso de privacidad, a fin de que pueda tomar decisiones informadas al respecto. El aviso de privacidad se pondrá a disposición del titular en sus dos modalidades simplificado e integral.

El aviso de privacidad simplificado debe señalar la siguiente información:

- La denominación completa del responsable.
- Las finalidades o usos que motivan el tratamiento de los datos personales, distinguiendo aquéllas que requieran del consentimiento del titular.
- Las transferencias de datos personales que, en su caso, se tengan previstas realizar y que requieran del consentimiento del titular.

- El sitio o medio donde el titular podrá consultar el aviso de privacidad integral.

Por su parte, el aviso de privacidad integral, además de señalar la información prevista en el aviso de privacidad simplificado, debe informar lo siguiente:

- El domicilio del responsable.
- Los datos personales que serán sometidos a tratamiento, identificando aquéllos que sean sensibles.
- El fundamento legal que faculta al sujeto obligado para llevar a cabo el tratamiento de los datos personales.
- Los mecanismos, medios y procedimientos disponibles para que los titulares puedan ejercer sus derechos ARCO.
- El domicilio de la Unidad de Transparencia del responsable.
- Las transferencias, nacionales y/o internacionales, de datos personales que, en su caso, efectúe y que no requieran de su consentimiento.
- Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

De manera adicional a los elementos señalados, el aviso de privacidad, de manera opcional, puede contener los siguientes elementos:

- Abreviatura o acrónimo por el cual se identifica al responsable (aviso de privacidad simplificado e integral).
- Datos de contacto del responsable (aviso de privacidad integral).
- Medios y/o fuentes de obtención de los datos personales (aviso de privacidad integral).
- Las transferencias, nacionales y/o internacionales, de datos personales que, en su caso, efectúe y que no requieran de su consentimiento (aviso de privacidad integral).
- La posibilidad que tiene el titular de ejercer su derecho a la portabilidad en el caso que sea posible (aviso de privacidad integral).

El aviso de privacidad debe caracterizarse por ser sencillo, con la información necesaria, expresado en lenguaje claro y comprensible y con una estructura y diseño que facilite su entendimiento, atendiendo al perfil de los titulares a quien irá dirigido, con la finalidad de que sea un mecanismo de información práctico y eficiente.

El responsable está obligado a poner a disposición del titular el aviso de privacidad simplificado en un primer momento, lo cual no le impide que pueda dar a conocer el aviso de privacidad integral desde un inicio, conforme a las siguientes reglas:

- De manera previa a la obtención de los datos personales cuando los mismos se obtengan directamente del titular, independientemente de los formatos o medios físicos y/o electrónicos utilizados para tal fin, o
- Al primer contacto con el titular o previo al aprovechamiento de los datos personales cuando éstos se hubieren obtenido de manera indirecta del titular.

El responsable debe publicar de manera permanente el aviso de privacidad integral, en el sitio o medio que se informe en el aviso de privacidad simplificado, a efecto de que el titular tenga la posibilidad de consultarlo en cualquier momento.

Asimismo, el responsable está obligado a difundir, poner a disposición o reproducir el aviso de privacidad, independientemente de la modalidad, en formatos físicos y electrónicos, ópticos, sonoros, visuales o a través de cualquier otra tecnología que permita su eficaz comunicación.

Cabe destacar, que el responsable tiene la obligación de poner a disposición del titular, un nuevo aviso de privacidad, en sus dos modalidades, cuando:

- Cambie su identidad.
- Requiera recabar datos personales sensibles adicionales a aquéllos informados en el aviso de privacidad original, los cuales no se obtengan de manera directa del titular y se requiera de su consentimiento para el tratamiento de éstos.
- Cambie las finalidades señaladas en el aviso de privacidad original.
- Modifique las condiciones de las transferencias de datos personales o se pretendan realizar transferencias no previstas inicialmente y el consentimiento del titular sea necesario.

Al respecto, en la evaluación de impacto presentada por la SESNA se advirtió lo siguiente:

> *"[...]*
> *Al ser una plataforma de interoperabilidad, **la PDN no genera ni almacena los datos**, sino que a través de servicios web o API´s, consulta la información de los servidores y las bases de datos de los generadores de la información, y los refleja en la Plataforma.*
>
> ***La forma más fácil de entender el funcionamiento de la PDN es pensar en cualquier plataforma de internet para reservar vacaciones (Por ejemplo; Expedia). Con tan solo introducir fechas, lugar y rango de precios, la plataforma de reservaciones genera una búsqueda de opciones de vuelos y hoteles. Estas plataformas no generan los datos por sí mismas, se comunican con otros sistemas para permitir al usuario consultar de manera uniforme entre miles de opciones de diversos proveedores de información, con tan solo un clic.***

> ***La PDN opera con una arquitectura basada en comunicaciones a través de internet, que permite consultar información desde diversos proveedores de información (entes de gobierno), en tiempo real y de manera estandarizada (en un mismo formato). Con el objetivo de incorporar datos a la PDN, los generadores de información deben establecer mecanismos tecnológicos que permitan la consulta de información desde la PDN hacia sus bases de datos.***
> *[...]" (Sic)*

En su documento de seguridad, la SESNA manifestó lo siguiente:

> *"La obtención de la información y datos personales para este Sistema de tratamiento de datos personales es realizada por La Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos, según corresponda. Estas autoridades son los encargados de obtener la información y, por lo tanto, de obtener el consentimiento respectivo de los titulares ya que la Plataforma Digital Nacional es una plataforma de interoperabilidad que no genera ni almacena los datos.*
> *[...]" (Sic)*

Conforme lo anterior, es preciso reiterar lo manifestado por la SESNA respecto de que no será quien obtenga directamente de los titulares, los datos personales que obran en cada uno de los sistemas que conforman la PDN, ya que dicha plataforma se integrará a partir de la información proporcionada por las autoridades que integran el SNA, a su vez proporcionada por lo proveedores de información (entes públicos) con atribuciones en la materia para brindar información de los sistemas S1, S2, S3 y S6.

De esta manera la SESNA obtendrá los datos personales que obran en cada uno de los sistemas que conforman la PDN de manera indirecta, a través de la comunicación de información que realizarán las autoridades que integran la SNA con los sistemas de la PDN.

En este sentido es preciso señalar que de conformidad con el artículo 26 de la Ley General, el responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto. Asimismo, el artículo 43 de los Lineamientos Generales establecen que se deberá poner a disposición el aviso de privacidad al titular de manera previa a la obtención de los datos personales, cuando los mismos se obtengan directamente del titular, o al primer contacto con el titular o previo al aprovechamiento de los datos personales, cuando éstos se hubieren obtenido de manera indirecta del titular.

En tal virtud, se advierte que si bien, el cumplimiento al principio de información se materializa a través del aviso de privacidad, también lo es que para dar a conocer este documento debe realizarse de

manera previa a la obtención de los datos personales o bien al primer contacto con el titular o previo al aprovechamiento de los datos personales.

Considerando lo anterior, se observa que en el caso específico estamos ante dos supuestos distintos en relación al cumplimiento del principio de información y las obligaciones que devienen del mismo, ya que, en un primer momento, la obtención directa de los datos personales de los titulares que obran en cada uno de los sistemas que conforman la PDN, la realiza los distintos entes públicos encargados de alimentar dicha plataforma.

En este sentido, la puesta a disposición de los avisos de privacidad correspondientes a cada uno de los sistemas actualiza el supuesto establecido en la fracción I del artículo 43 de los Lineamientos Generales, en relación con el momento en el cual se debe poner a disposición de los titulares el aviso de privacidad en cualquiera de sus dos modalidades, esto es de manera previa a la obtención de datos personales, cuando los mismos se obtengan de manera directa del titular.

Por lo tanto y en esta lógica, son los entes públicos los responsables de informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, en la modalidad, medios que cada una de las autoridades determine, así como en atención a los momentos de puesta a disposición según corresponda.

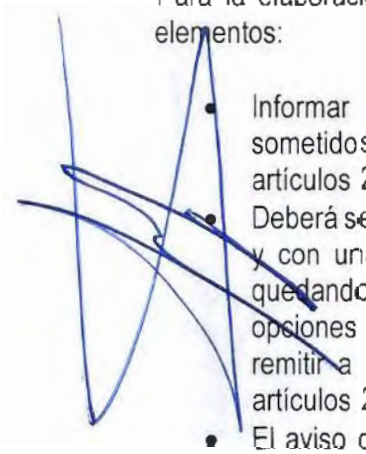
Ahora bien, por lo que hace al segundo supuesto, la SESNA como responsable del tratamiento que realice en la PDN, actualizaría el supuesto previsto en la fracción II del artículo 43 de los Lineamientos Generales, toda vez que como ya fue referido en múltiples ocasiones, los datos personales se obtienen de manera indirecta de los titulares, por lo que en este supuesto el aviso de privacidad correspondiente deberá ponerse a disposición de los titulares al primer contacto con estos o previo al aprovechamiento de los datos personales.

Respecto a lo anterior, de las manifestaciones vertidas por la SESNA así como de la información que se acompaña en la presentación de la evaluación de impacto que nos ocupa, es posible advertir que exista necesariamente un contacto o interacción directa con los titulares de los datos personales, por lo que independientemente de dicha consideración, la SESNA aún estaría obligada a cumplir con el principio de información, toda vez que se constituye como responsable del tratamiento de datos personales al permitir la interoperabilidad, acceso y consulta, de la información y sistemas contenidos en la PND, poniendo a disposición un aviso de privacidad previo al aprovechamiento de los datos personales, es decir, previo a que dé inicio al tratamiento habilitando la funcionalidad del acceso de los distintos sistemas por medio de las APIs.

En virtud de lo anterior, este Instituto determina que la SESNA está obligada a poner a disposición un aviso de privacidad del tratamiento de datos personales que realice con la implementación de la PDN, el cual se trata de un documento diferente a los Términos y Condiciones de Uso de la PDN, que fueron referidos en la evaluación de impactado presentada.

Por lo tanto, la SESNA estaría en el supuesto de responsable para cumplir con el principio de información y poner a disposición, el aviso de privacidad correspondiente, en el que se informe al titular la existencia y características principales del tratamiento al que serán sometidos sus datos personales de conformidad con a lo dispuesto en los artículos 26, 27 y 28 de la Ley General y 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, y 49 de los Lineamientos Generales.

Para la elaboración del aviso de privacidad simplificado, la SESNA deberá incluir los siguientes elementos:



- Informar al titular la existencia y características principales del tratamiento al que serán sometidos sus datos personales a través de la PDN de conformidad con lo dispuesto en los artículos 26 de la Ley General y 26 de los Lineamientos generales.
- Deberá ser sencillo, con la información necesaria, expresado en lenguaje claro y comprensible y con una estructura que facilite su entendimiento, de acuerdo al perfil de los titulares, quedando prohibido, el uso de frases inexactas, incluir textos o formatos que induzcan a elegir opciones en específico, marcar previamente casillas relacionadas con el consentimiento, o remitir a documentos que no estén disponibles, de conformidad con lo dispuesto en los artículos 26 de la Ley General y 28 de los Lineamientos generales.
- El aviso de privacidad deberá difundirse, ponerse a disposición, o reproducirlo en formatos físicos, electrónicos, ópticos, sonoros, visuales o a través de cualquier tecnología, de conformidad con lo dispuesto en los artículos 27, fracción I de la Ley General y 30 de los Lineamientos generales.
- Se deberá señalar la denominación completa de la SESNA de conformidad con lo dispuesto en los artículos 27, fracción I de la Ley General y 30 de los Lineamientos generales.
- Se deberán indicar de manera específica las finalidades del tratamiento de datos personales, con base en lo mencionado a lo largo del presente dictamen conforme a lo dispuesto en los artículos 27, fracción II de la Ley General y 31 de los Lineamientos generales.
- Se deberá señalar si la SESNA realizará transferencias de datos personales a que se refiere el artículo 3, fracción XXXII de la Ley General, atendiendo a lo dispuesto en los artículos 27, fracción III de la Ley General y 32 de los Lineamientos generales.

- Se deberá incluir o informar el mecanismo o medio habilitado para recabar el consentimiento del titular atendiendo a lo dispuesto en los artículos 27, fracción IV de la Ley General y 33 de los Lineamientos generales.
- Se deberá identificar claramente el medio que habilitará la SESNA para que los titulares puedan conocer el aviso de privacidad integral, de conformidad con los artículos 27, fracción V de la Ley General y 34 de los Lineamientos Generales.

Respecto al aviso de privacidad integral, la SESNA además de los elementos señalados para el aviso de privacidad simplificado deberá incluir lo siguiente:

- Se deberá mencionar el domicilio de la SESNA a que se refieren los artículos 28, fracción I de la Ley General y 37 de los Lineamientos Generales.
- Se deberá indicar la totalidad de los datos personales que serán objeto de tratamiento a través de la PDN conforme a lo dispuesto en los artículos 28, fracción II de la Ley General y 38 de los Lineamientos Generales y conforme los argumentos vertidos en el principio de proporcionalidad del presente dictamen.
- Se deberán señalar los fundamentos legales que facultan a la SESNA para llevar a cabo el tratamiento a través de la PDN según lo dispuesto en los artículos 28, fracción III de la Ley General y 38 y 39 de los Lineamientos Generales.
- Se deberán indicar de manera específica las finalidades del tratamiento de datos personales, con base en lo mencionado en el presente dictamen y conforme a lo dispuesto en los artículos 27, fracción II y 28, fracción IV de la Ley General y 31 y 35 de los Lineamientos Generales.
- Describir puntualmente el procedimiento para el ejercicio de derechos ARCO, o bien remitir al titular a los medios que tenga disponibles para que conozca dicho procedimiento, de conformidad con lo establecido en el artículo 28 fracción V de la Ley General y 40 de los Lineamientos Generales.
- Los requisitos que deberá contener la solicitud para el ejercicio de los derechos ARCO a que se refiere el artículo 52 de la Ley General y 40 fracción I de los Lineamientos generales.
- Informar a los titulares en el aviso de privacidad integral los medios habilitados para dar respuesta a las solicitudes para el ejercicio de derechos ARCO; la modalidad o medios de reproducción de los datos personales; los plazos establecidos dentro del procedimiento, los cuales no deberán contravenir lo previsto en los artículos 51, 52, 53 y 54 de la Ley General; el derecho que tiene el titular de presentar un recurso de revisión ante el Instituto en caso de estar inconforme con la respuesta; lo anterior, de conformidad con los artículos 28, fracción V de la Ley General y 40 fracciones IV, V, VI y VII de los Lineamientos Generales.

- Se deberá señalar los datos de la Unidad de Transparencia de la SESNA, conforme a lo dispuesto en los artículos 28, fracción VI de la Ley General y 41 de los Lineamientos Generales.
- Se deberá identificar claramente el medio que habilitará la SESNA para dar a conocer los cambios en el aviso de privacidad integral, de conformidad con los artículos 28, fracción VII de la Ley General y 42 de los Lineamientos Generales.

Por otro lado, se advierte que, en torno a los objetivos que persigue la PDN, está la de permitir que diferentes usuarios de la PDN tengan acceso a la plataforma y puedan consultar la información dentro de cada uno de los sistemas de información, para las diferentes funcionalidades y alcances de acuerdo con cada perfil.

En este sentido, es importante señalar lo establecido por la SESNA en su evaluación de impacto en la protección de datos personales, la cual dice a la letra:

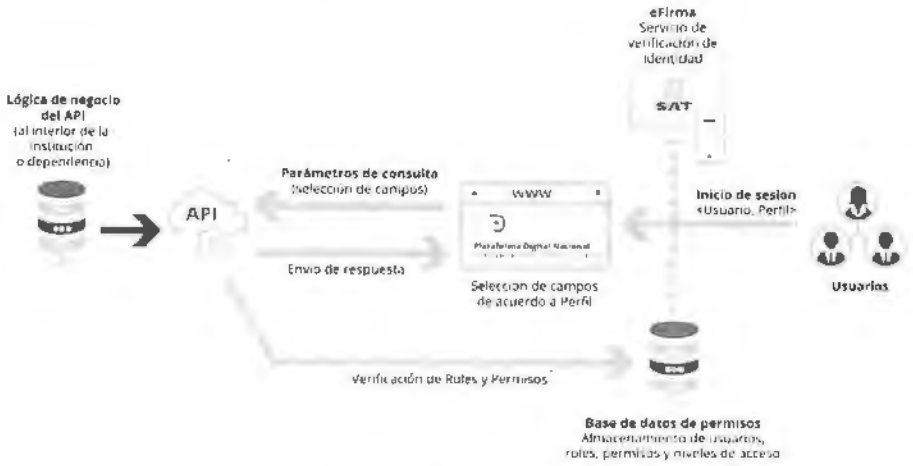
> *"4. **Acceso no autorizado**: Es fundamental mencionar que **el acceso a los datos reservados se realizará con base en los permisos que el Comité Coordinador del SNA y con base en las atribuciones que la legislación aplicable confiere a aquellos** que pueden consultar los datos reservados. En caso de que se registre un acceso no autorizado, se debe identificar de dónde provino y cómo fue el acceso.*
>
> ***A través de usuario registrado y con privilegios. Al generar un acceso mediante usuario y contraseña a la PDN, que tenga privilegios para la consulta de información confidencial**, se le confiere la completa responsabilidad al usuario, del buen uso, resguardo y confidencialidad de sus datos de usuario y contraseña. En caso de existir el robo o uso ilegal de su usuario y contraseña, el usuario debe notificar inmediatamente al personal de la SESNA para bloquear esa cuenta. Se hará un rastreo de los datos que se consultaron, la fecha y la hora. Se notificará al usuario sobre la información que se consultó.*
>
> ***Resguardo de usuarios y contraseñas para acceder a datos reservados: Las credenciales, listas de permisos y contraseñas se resguardarán en una Base de Datos segura que podrá ser consultada únicamente por los Encargados y el equipo administrador de la PDN.** La Base de Datos segura contará con el soporte de las cuatro capas de seguridad antes mencionadas (**Sistema Operativo, Aplicaciones, Segmento de red y Red perimetral**). Asimismo, en la Base de Datos las contraseñas de acceso se encontrarán cifradas para evitar que puedan ser visibles a ojo humano o utilizadas para acceder al sistema en el supuesto caso de que un atacante llegara a sustraerlas de la PDN."*

Aunado a lo anterior, en su respuesta a la información adicional la SESNA indicó:

> *"Respecto a la información contenida en el Sistema 1, se debe dividir la información en pública y reservada, de acuerdo con lo aprobado por el Comité Coordinador2 -del que forma parte el INAI-. En esta etapa de la PDN solo se cuenta con información de carácter público. Hasta que no se apruebe y publique el catálogo de perfiles -que establecerá quiénes son los usuarios que podrán acceder a la información reservada, conforme a la normativa aplicable- la PDN no permitirá la consulta y el intercambio de los datos reservados.*

Se aclara que, al momento de la presentación de esta Evaluación, este catálogo de perfiles es encuentra en elaboración."

Asimismo, conviene traer a colación el flujo de la operación de **la PDN:**



Al respecto, se advierte que, como parte de las finalidades de la propia PDN, es dar la posibilidad de acceder y consultar la información que obran en los sistemas que la conforman, por lo que es importante advertir que, como parte de dicha funcionalidad se permitirá el acceso a datos reservados que se realizará con base en los permisos que el Comité Coordinador del SNA y con base en las atribuciones que la legislación aplicable confiere a aquellos que pueden consultar los datos reservados.

Conforme a lo anterior, el acceso a este tipo de información reservada se advierte que se realizará a través de generar un acceso mediante usuario y contraseña a la PDN, que tenga privilegios para la consulta de información confidencial.

Asimismo, se puede identificar que el resguardo de usuarios y contraseñas para acceder a datos reservados: es decir, las credenciales, listas de permisos y contraseñas se resguardarán en una Base de Datos que podrá ser consultada únicamente por los encargados de proporcionar información a los sistemas de la PDN y el equipo administrador de la PDN. No obstante, la SESNA no señala mayor información sobre dicha base de datos.

Por último, se puede advertir que, respecto de la información contenida en el S1, ésta se encuentra dividida en pública y reservada, de acuerdo con lo aprobado por el Comité Coordinador. Y se indica

que en la etapa en la que se encuentra actualmente la PDN solo se cuenta con información de carácter público y será hasta que se apruebe y publique el catálogo de perfiles -que establecerá quiénes son los usuarios que podrán acceder a la información reservada, conforme a la normativa aplicable-, en términos de lo establecido en los artículos 3, fracción IV y 18 de las Bases para el funcionamiento de la PDN; no permitirá la consulta y el intercambio de los datos reservados en dicha plataforma.

En este sentido, la SESNA declaró que, al momento de la presentación de esta Evaluación, este catálogo de perfiles se encuentra en elaboración, por lo cual se puede concluir que esta funcionalidad no se encuentra operando actualmente.

Tan es así que, al realizar las pruebas de ingreso a la PDN a través del vínculo electrónico https://www.plataformadigitalnacional.org/ por parte de este Instituto, fue posible advertir que, para acceder y consultar la información que ya yace en los sistemas 1, 2, 3 y 6, no se solicita ningún tipo de procedimiento de inicio de sesión o registro.

Por lo anterior, este Instituto se advierte que para el uso o consulta de datos reservados que obran en la PDN, habrá un procedimiento de inicio de sesión a través de un usuario previamente registrado. Sin embargo, de la información proporcionada por la SESNA, si bien, se señala que la PDN no permitirá la consulta y el intercambio de los datos reservados en tanto no se apruebe y publique el catálogo de perfiles que se mandata en las Bases de funcionamiento de la PDN en el que se determinará el listado y descripción de los perfiles de usuarios existentes para distinguir los niveles de acceso, gestión y uso de la información de los sistemas de la Plataforma, lo cierto es que tampoco se brinda mayor información sobre qué datos personales serán los que se requerirán para el registro de los usuarios con privilegios para acceder a información reservada, ni se estipula mayor información sobre las bases de datos en las que se resguardarán las credenciales, listas de permisos y contraseñas.

En este sentido, se puede advertir que un procedimiento en el cual se requiera iniciar sesión conlleva necesariamente un registro previo por parte del usuario mediante el cual se proporcionen datos requeridos para establecer un usuario, así como la generación de una contraseña, por lo que, se estaría configurando un tratamiento de datos personales a través de la PDN, al recabar datos personales a efecto de realizar un registro. Asimismo, puede suponerse que este tipo de registros podrían ser llevados a cabo por personas físicas, relativas a servidores públicos pertenecientes a las autoridades usuarias facultadas para acceder a información de la PDN que requiera este registro previo o inclusive por personas físicas en representación de particulares sancionados o inhabilitados de acuerdo con los perfiles de datos personales previamente señalados.

Por lo tanto, es preciso señalar que al implementar esta funcionalidad de inicio de sesión para el acceso de determinados perfiles de usuarios que así se determine por la SESNA, actualizaría un

tratamiento de datos personales, además de que la obtención de estos será realizada directamente al titular, por lo que la SESNA estaria en el supuesto de responsable para cumplir con el principio de información y poner a disposición, previo registro de los usuarios, el aviso de privacidad correspondiente, en el que se informe al titular la existencia y caracteristicas principales del tratamiento al que serán sometidos sus datos personales de conformidad con a lo dispuesto en los artículos 26, 27 y 28 de la Ley General y 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, y 49 de los Lineamientos Generales.

Finalmente, y de conformidad con lo anterior, respecto de la emisión de usuarios previamente registrados e identificados, es importante que la SESNA considere la protección de datos generados a partir de la navegación de los usuarios dentro de la plataforma. Lo anterior, toda vez que, en el entendido de que habrá un registro de determinados perfiles de usuario para el uso de la PDN, por lo que los datos generados a través de la navegación de dichos usuarios de la plataforma o en caso de utilizar tecnologías de rastreo como las cookies, podrán constituirse como datos personales, entendiendo dato personal como toda información concerniente a una persona física identificada o identificable de conformidad con el artículo 3, fracción VIII de la Ley General.

De esta manera, los usuarios que se registren serán personas físicas que proporcionarán datos concernientes, a su persona para realizar el registro e iniciar sesión, por lo que los datos obtenidos de su navegación por la plataforma se actualizarán como datos personales y por ende se podrá considerar que existe un tratamiento de datos personales pues el usuario podrá ser identificado por un nombre o demás datos que haya proporcionado al momento del registro.

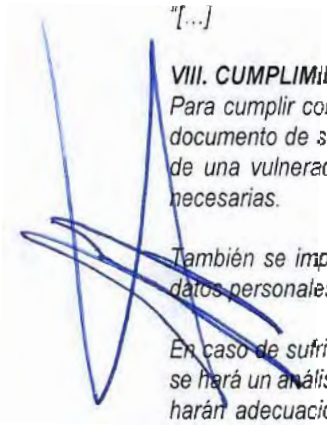
Por lo cual, se recomienda a la SESNA, realizar las actividades que le corresponden en torno al principio de información a través de la emisión de un aviso de privacidad en el que se señale a los titulares de datos personales que podrán llevarse a cabo dichos tratamientos a través de la información generada por la navegación en la plataforma, así como los alcances y finalidades para los cuales serán tratados, previo al registro que realicen; el cual, debería considerar las interacciones con los diversos sistemas, subsistemas y componentes con los que interactúa, tanto en lo técnico, como en cuanto al contenido de los diversos avisos de privacidad que eventualmente deberían reconocer las transferencias que se realicen en el marco de la PDN.

1.8. Principio de responsabilidad

Los articulos 29 y 30 de la Ley General, 46, 47, 48, 49, 50, 51 y 52 de los Lineamientos generales, de los que se desprende que el responsable está obligado a implementar mecanismos que permitan acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General como son, de manera enunciativa más no limitativa, las siguientes:

- Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior del sujeto obligado.
- Establecer un sistema de supervisión y vigilancia interna y/o externa para comprobar el cumplimiento de las políticas de protección de datos personales.
- Diseñar, desarrollar e implementar políticas públicas, programas, servicios o sistemas de conformidad con las disposiciones previstas en la Ley General.
- Garantizar que las políticas públicas, programas, servicios o sistemas cumplan por defecto con las obligaciones previstas en la Ley General.

Sobre el particular, la SESNA manifestó lo siguiente:



"[...]

VIII. CUMPLIMIENTO NORMATIVO

Para cumplir con los deberes legales[22] en materia de protección de datos personales se elaboró un documento de seguridad el cual será revisado anualmente para detectar áreas de mejora o, en caso de una vulneración, a revisión se hará inmediatamente para implementar las medidas correctivas necesarias.

También se implementará un programa de capacitación especializado en materia de protección de datos personales para todas las personas servidoras públicas que integran la USTPDN.

En caso de sufrir algún incidente que ponga en riesgo u exponga la información contenida en la PDN se hará un análisis inmediato de las medidas de seguridad para detectar vulnerabilidades. Además, se harán adecuaciones al plan de trabajo establecido en el documento de seguridad para incorporar acciones preventivas y correctivas.
[...] (Sic)

En su Documento de seguridad, la SESNA manifestó lo siguiente:

*"8. **MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD***
Como mecanismos de monitoreo, se utilizan las auditorías que registran los accesos a sistemas y datos de todos los usuarios con el objetivo de detectar posibles riesgos de seguridad.
Los registros de auditoría deberán incluir:

1. Identificación del usuario.
2. Fecha de inicio y fin.
3. Registros de intentos exitosos y fallidos de acceso a los sistemas.
4. Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere, la periodicidad de las revisiones se realizará de manera semestral.

Monitoreo del Uso de los Sistemas

Se realiza un monitoreo sobre el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente. La periodicidad de las revisiones se realizará de manera semestral.

Todo el personal de la USTPDN debe conocer el alcance preciso del uso adecuado de los recursos informáticos, así como las actividades que pueden ser objeto de control y monitoreo.

Entre los eventos que deben tenerse en cuenta para el control y monitoreo de los sistemas, se enumeran las siguientes:

1. Acceso no autorizado, incluyendo detalles como:
- *a) Identificación del usuario.*
- *b) Fecha y hora de eventos clave.*
- *c) Tipos de eventos.*
- *d) Archivos a los que se accede.*

2. Todas las operaciones con privilegio, como:
- *a) Uso de cuenta de administrador.*
- *b) Inicio y cierre del sistema.*
- *c) Conexión y desconexión de dispositivos de ingreso y salida de información o que permitan copiar datos.*
- *d) Cambio de fecha/hora.*
- *e) Cambios en la configuración de la seguridad.*
- *f) Alta de servicios.*

3. Intentos de acceso no autorizado, como:
- *a) Intentos fallidos.*
- *b) Violaciones de accesos y notificaciones para "Gateways" y "Firewalls".*
- *c) Alertas de sistemas de detección de intrusiones.*

4. Alertas o fallas de sistema como:
- *a) Alertas o mensajes de consola.*
- *b) Excepciones del sistema de registro.*
- *c) Alarmas del sistema de administración de redes.*

Registro y Revisión de Eventos

Registro y revisión de los eventos de auditoria, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados.

La periodicidad de dichas revisiones es de manera semestral, utilizando herramientas especificas para auditoria o utilitarios adecuados para llevar a cabo el control de los registros.

Las herramientas de registro deberán contar con los controles de acceso necesarios, a fin de garantizar que no ocurra:

> ***9. PROGRAMA GENERAL DE CAPACITACIÓN***
> *La Unidad de Transparencia difundirá su programa de capacitación y actualización para los servidores públicos de la SESNA en materia de protección de datos personales al que está obligado a establecer el Comité de Transparencia de conformidad con lo dispuesto en el artículo 84 fracción VII de la LGPDPPSO, a efecto de que dichos servidores públicos se capaciten respecto de la protección de datos personales y ejercicio de derechos ARCO. También se desarrollará un programa de capacitación especializado para las personas servidoras públicas que sean responsables del tratamiento y protección de datos personales.*
>
> *Adicionalmente a los cursos impartidos por el INAI, se prevé la contratación de capacitadores externos para garantizar un mayor nivel de especialización en las prácticas y conocimiento de los servidores públicos responsables del tratamiento de los datos personales."*

Asimismo, respecto del requerimiento de información adicional se advierte lo siguiente:

> *"**16.** Se realizarán revisiones anuales del Documento de Seguridad, informes de la operación de la PDN e incidentes para identificar áreas de mejora. En caso de existir suficiencia presupuestaria se realizarán auditorías externas para analizar el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en la Ley General." (Sic).*

Al respecto, es importante mencionar que para dar cumplimiento a este principio es necesario demostrar la realización de una serie de acciones que permitan acreditar el cumplimiento de las obligaciones previstas en a Ley General, los Lineamientos generales y demás normatividad aplicable en la materia.

Por lo cual, conviene manifestar que las obligaciones del principio de responsabilidad van más allá de los programas de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales que puedan impartirse al personal de la SESNA, del establecimiento de los mecanismos de monitoreo o revisión de las medidas de seguridad o las auditorías supeditadas a la existencia de suficiencia presupuestaria, lo cual, de ninguna manera significa que no sean valiosos, pero que son sólo una parte del cúmulo de obligaciones que se esperan para el cumplimiento del principio que se analiza.

Asimismo, es importante distinguir entre el objetivo y alcance del documento de seguridad entendido como el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas, administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee conforme a lo señalado en el artículo 3, fracción XIV de la Ley General, de las obligaciones que el responsable está obligado a llevar a cabo para el cumplimiento de los principios, deberes y demás obligaciones establecidas en dicho ordenamiento, así como para rendir cuentas sobre el tratamiento de datos personales en su posesión al titular e Instituto de acuerdo con el artículo 29 de la Ley General.

Tomando en cuenta esta fundamental distinción, se concluye que fue posible advertir la implementación de algunos mecanismos para el cumplimiento de responsabilidad, no obstante, no fue posible advertir, a partir de las manifestaciones de la SESNA, las acciones concretas que sujeto obligado llevarían a cabo para el cumplimiento de esta obligación, tampoco se aportó ninguna evidencia que acredite de manera fehaciente la implementación de los mismos.

Es por ello, que el Instituto determina que la SESNA está obligada a implementar los mecanismos y controles concretos que consideren pertinentes y que tengan por objeto acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General, los Lineamientos generales y demás normatividad aplicable, como son, de manera enunciativa más no limitativa, los siguientes:

- Destinar recursos autorizados para la instrumentación de programas y políticas de protección de datos personales, conforme a lo dispuesto en el artículo 47 de los Lineamientos Generales.
- Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización de la SESNA de acuerdo con el artículo 47 de los Lineamientos Generales.
- Poner en práctica un programa de capacitación y actualización en materia de protección de datos personales dirigido a su personal y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales, en términos de lo previsto en el artículo 48 de los Lineamientos Generales.
- Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran, atendiendo a lo indicado en el artículo 49 de los Lineamientos Generales.
- Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorias, para comprobar el cumplimiento de las políticas de protección de datos personales, conforme a lo dispuesto en el artículo 49 de los Lineamientos Generales.
- Establecer procedimientos para recibir y responder dudas y quejas de los titulares, en términos de lo señalado en el artículo 50 de los Lineamientos Generales.

De manera particular, la SESNA deberá poner especial atención a la implementación de los mecanismos para la protección de datos personales por diseño y por defecto, en la implementación de la PDN, a saber:

- Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la Ley

General y las demás que resulten aplicables en la materia, en términos de lo dispuesto en el artículo 51 de los Lineamientos Generales.

Lo anterior, por medio de la aplicación de medidas de carácter administrativo, técnico, físico u otras de cualquier naturaleza que, desde el diseño, le permitan aplicar de forma efectiva el cumplimiento de los principios, deberes y demás obligaciones previstas en la Ley General y los Lineamientos Generales, en sus políticas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales.

- Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la Ley General y las demás que resulten aplicables en la materia, de acuerdo con lo estipulado en el artículo 52 de los Lineamientos Generales.

Para lo cual, el responsable deberá aplicar medidas técnicas y organizativas apropiadas y orientadas a garantizar que, por defecto, sólo sean objeto de tratamiento los datos personales estrictamente necesarios para cada uno de los fines específicos del tratamiento.

Lo anterior, considerando el desarrollo tecnológico y las técnicas existentes; la naturaleza, contexto, alcance y finalidades del tratamiento de los datos personales, las atribuciones y facultades de la SESNA y demás cuestiones que se considere convenientes.

2. Deber de seguridad

2.1. Tecnología utilizada

La Ley General, señala en su artículo 32 lo siguiente:

> *"**Artículo 32.** Las medidas de seguridad adoptadas por el responsable deberán considerar:*
> *[...]*
>
> *III. El desarrollo tecnológico;*
> *[...]"(Sic).*

Por su parte, las Disposiciones administrativas, en su artículo 10, fracción XII señalan que, en la descripción de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales y que pretenda poner en operación o modificar, el responsable deberá indicar, lo siguiente:

"[...]

XII. *La tecnología que se pretende utilizar para efectuar el tratamiento intensivo o relevante de datos personales;*
[...]" (Sic)

Al respecto, la SESNA informó en la evaluación de impacto en la protección de datos personales lo siguiente:

S1
"II.7 Tecnología utilizada
La tecnología utilizada para el S1 es la misma que se utiliza para el funcionamiento general de la PDN, esto es, un sistema de interoperabilidad que a través de servicios web o API´s, consulta la información de los servidores y las bases de datos de los generadores de la información, en el caso concreto, la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos, y los refleja en la PDN.
Como lo establecen las Bases para el Funcionamiento de la Plataforma Digital Nacional, la estandarización de la información es uno de los requerimientos normativos y operativos para lograr la interoperabilidad de los datos del S1 con la PDN.
El artículo 6 establece:
"Para el correcto funcionamiento de cada uno de los sistemas, la Secretaría Ejecutiva emitirá los protocolos, estándares, reglamentos, especificaciones técnicas y cualquier normativa necesaria para la colaboración, provisión de datos y acciones para cumplir con las Bases, los cuales serán obligatorios para todos los proveedores, concentradores y encargados a nivel federal, estatal y municipal."
La SESNA publicó en octubre de 2019 el estándar de datos y los diccionarios de datos y catálogos de valores para el S1, que encuentran disponibles en: https://plataformadigitalnacional.org/declaraciones/especificaciones"

S2
"III.7 Tecnología utilizada
La tecnología utilizada para el S2 es el mismo que se utiliza para el funcionamiento de la PDN, esto es, un sistema de interoperabilidad que a través de servicios web o API´s, consulta la información de los servidores y las bases de datos de los generadores de la información y los refleja en la PDN."

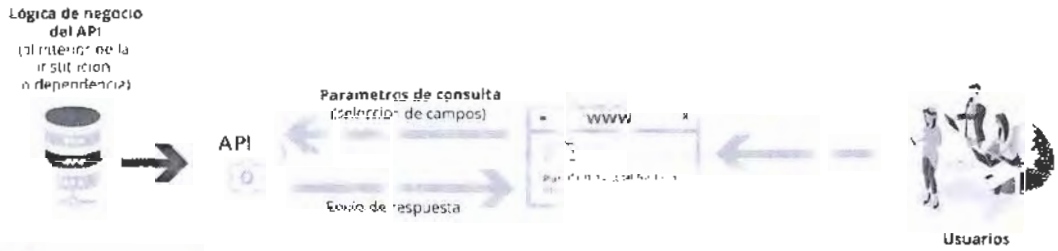
S3
IV.7 Tecnología utilizada
Interoperabilidad que a través de servicios web o API´s, consulta la información de los servidores y las bases de datos de los generadores de la información y los refleja en la PDN."

S4
V.7 Tecnología utilizada
La tecnología utilizada para el S6 es la misma que se utiliza para el funcionamiento general de la PDN, esto es, un sistema de interoperabilidad que a través de servicios web o API´s, consulta la información de los servidores y las bases de datos de los generadores de la información y los refleja en la PDN.

[...]"

En su respuesta al requerimiento de información se señaló lo siguiente:

"La PDN trabaja bajo un modelo de interoperabilidad de sistemas de información, es decir, bajo esquemas de comunicación digital que permiten la compatibilidad de la información compartida. Para lograr la interoperabilidad, se diseñaron y publicaron estándares de datos para los sistemas 1, 2, 3 y 6 de la PDN y se emitieron las especificaciones técnicas para el intercambio de información a través de APIs tipo REST



Como se aprecia en la imagen anterior, bajo este esquema los entes públicos son los responsables de asegurar la integridad y seguridad de su información, así como de mantener disponible la comunicación con la PDN 24/7, los 365 días del año.

Bajo esta línea de trabajo, los entes públicos interesados en incorporar información a la PDN pasan por diferentes etapas de integración para incorporar sus datos a la PDN:

*1. **Pruebas en ambiente de desarrollo.** Los entes públicos envían una solicitud de conexión debidamente requisitada y bajo el formato emitido por la PDN16. En esta etapa se llevan a cabo pruebas funcionales y de conectividad en ambiente de desarrollo, el cual deberá contar con datos ficticios para la realización de las pruebas. Dichas pruebas se encuentran descritas y disponibles en la página de la PDN.*

*2. **Pruebas en ambiente de producción.** Una vez que aprobaron la etapa anterior, los entes públicos interesados en incorporar información a la PDN deberán enviar una solicitud de conexión para dicho ambiente, el cual deberá contar con los datos reales que serán suministrados a la PDN, los cuales no deberán contar datos reservados, y los endpoints de sus servicios deberán contar con un certificado SSL para cifrar las comunicaciones. En esta etapa se llevarán a cabo pruebas funcionales, de conectividad y de nivel de servicio. En caso de que el sujeto obligado cuente con ella, se establece la comunicación con su VPN.*

*3. **Integración a PDN y pase a producción.** Una vez que se han aprobado las pruebas en ambiente productivo, el equipo de la PDN integra finalmente el servicio a los buscadores correspondientes de la PDN.*

*4. **Mantenimiento.** El ente público interesado en incorporar su información a la PDN se compromete a dar mantenimiento a sus servicios en caso de cualquier actualización en los estándares de datos así como de las especificaciones técnicas emitidas para la PDN. Además, se establece el enlace correspondiente para la atención de cualquier falla y/o intermitencia del servicio.*

Durante las etapas de integración, el personal de la USTPDN de la SESNA se encarga de recibir, atender y evaluar las solicitudes, así como de llevar a cabo la integración con la PDN una vez que han superado la etapa 1 y 2 exitosamente.
Los Planes de prueba para verificar el funcionamiento de las APIs se encuentran disponibles en las siguientes direcciones:

- ***Sistema 1:*** *https://drive.google.com/file/d/1HZailvIOV77By1JwQKWXGTungYRBFmHi/view*

- ***Sistema 2:*** *https://drive.google.com/file/d/1ooAuvc1kNMiftE_R1yRgIC6Ok9bIIx8U/view*

- ***Sistema 3:***
Servidores públicos sancionados:
https://drive.google.com/file/d/1m6bHg8rgeTl_v48BpByDjgxeF2fIIve/view
Particulares sancionados:
https://drive.google.com/file/d/15mPsTLuW6u97cRMxBaEP8YCkAZnX32v-/view

[...]" (Sic)

Al respecto, en la respuesta del requerimiento número 4 el cual versa sobre el artículo 15 fracción XII, se observa que la SESNA hace alusión a la tecnología de interoperabilidad en el esquema que presenta dentro de la documentación, es así que, la plataforma no genera o almacena datos personales de los sistemas, aunque, genera otro tipo de datos por la interconexión de sistemas y por la propia navegación que realiza un usuario, en los documentos entregados se indica que como tal la plataforma es un mecanismo de conexión, aunque, no se muestra evidencia que compruebe que los datos de navegación del usuario son únicamente utilizados con fines estadísticos y para control de posibles errores por el uso de la plataforma.

De esta manera, a partir de la descripción de la relación, conexión, características y otros elementos de los sistemas que conectan con la plataforma, se recomienda dejar evidencia de que cada sistema es responsabilidad del propietario, así como resultados de pruebas que demuestren la seguridad de la comunicación entre sistemas y plataforma que indiquen que no hay riesgos hacia los sistemas por la comunicación desde la plataforma, garantizando la integridad de los datos que se consultan y las bases de datos del propietario, dejando claro que la plataforma no representa riesgos y que, las amenazas que pudieran presentarse son conocidas y se pueden contener en caso de alguna vulneración.

2.2. Medidas de seguridad de carácter administrativo, físico y técnico que se pretenden para la PDN

Con relación a las medidas de seguridad administrativas, físicas y técnicas, los artículos 31 y 34 de la Ley General establecen que:

> *"**Artículo 31.** Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá 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 su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.*
>
> ***Artículo 34.** Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán ser documentadas y contenidas en un sistema de gestión.*
> *[...]" (Sic)*

Asimismo, el artículo 55 de los Lineamientos generales señalan que:

> *"**Deber de seguridad***
> ***Artículo 55.** El responsable deberá establecer y mantener medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales en su posesión de conformidad con lo previsto en los artículos 31, 32 y 33 de la Ley General, con el objeto de impedir, que cualquier tratamiento de datos personales contravenga las disposiciones de dicho ordenamiento y los presentes Lineamientos generales.*
>
> *Las medidas de seguridad a las que se refiere el párrafo anterior constituyen mínimos exigibles, por lo que el responsable podrá adoptar las medidas adicionales que estime necesarias para brindar mayores garantías en la protección de los datos personales en su posesión."*

Por otro lado, las Disposiciones Administrativas, en su artículo 15, fracción XIII establecen que, en la descripción de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales y que pretenda poner en operación o modificar, el responsable deberá indicar, lo siguiente:

> *"XIII. Las medidas de seguridad de carácter administrativo, físico y técnico a implementar de conformidad con lo previsto en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables." (Sic)*

Al respecto, la SESNA manifestó lo siguiente:

> *"[...]*
>
> ***Medidas de seguridad***
> *Los mecanismos de seguridad que se ejecutan para garantizar la seguridad de los datos consultables a través de la PDN, especialmente los datos reservados, son los siguientes:*

1. Transferencias y Remisiones. - Se realizan de conformidad con lo siguiente:

o De traslado sobre redes electrónicas: La SESNA utiliza una red privada virtual bajo el protocolo IPSec para establecer un canal seguro de comunicación entre los Encargados y la PDN.

o El Encargado y la SESNA cuentan con sistemas y/o protocolos de detección de intrusos (IDS) para asegurar que las transferencias se llevan a cabo únicamente entre el Encargado y la PDN, identificando cualquier actividad o flujo de información atípicos. Las transmisiones se registran en una bitácora electrónica que se controla de manera interna.

o La selección de la información que se transfiere entre Encargados y la SESNA se da con base en las consultas realizadas por los usuarios de la PDN. Por ende, las transferencias de información de las bases de datos del Encargado a la PDN únicamente se dan como resultado de una consulta.

o La consulta de información a través de la PDN puede hacerse anónimamente siempre que se trate de información no reservada.

o Al generar una consulta pública en la PDN, únicamente se transfiere la información no reservada de los Encargados. En ese sentido, los Encargados deberán evitar exponer registros completos, con información adicional a la que se puede obtener de manera pública y anónima.

o La consulta de información reservada en ningún caso se puede realizar de manera anónima y se requiere de permisos especiales para que el Encargado y la PDN permitan su acceso.

2. Bitácoras para accesos y operación cotidiana.

o La PDN permite la consulta de información no reservada de manera pública y anónima, por lo cual, se cuenta con un registro con fines estadísticos que permite identificar búsquedas frecuentes y otras métricas de uso.

o Para el acceso a la información reservada, será necesario iniciar sesión en la PDN a través de un usuario y contraseña. También, en una segunda etapa se contará con la opción de inicio de sesión a través de la firma electrónica.

o El acceso a la información reservada se encuentra restringido a los servidores públicos que tengan las facultades y atribuciones legales para poder consultar esta información reservada. Todo acceso a información reservada deberá ser registrado por el Encargado y la PDN.

o Los Encargados y la SESNA contarán con una base de datos que incluirá la información necesaria para identificar a los servidores públicos y sus respectivas facultades para acceso a la información reservada.

o El registro del acceso a la información reservada deberá contener al menos los siguientes datos:

- *Usuario que realizó la consulta*
- *Nombre del servidor público*
- *Datos de adscripción del servidor público (Institución, unidad, etc.)*

- *Parámetros de consulta (el objeto de la búsqueda)*
- *Fecha de la consulta*

3. Registro de incidentes. - En caso de suceder algún incidente que implique la divulgación de información reservada o el mal uso de los datos personales consultables en la PDN:

- *El incidente se documenta y se agrega a la bitácora en donde se registra cualquier tipo de incidente de esta índole.*
- *Se dará aviso al Encargado de la generación e interoperabilidad de los datos acerca del incidente en cuestión para tomar las medidas correctivas adecuadas.*

4. Los Encargados y la PDN realizarán periódicamente verificaciones a sus sistemas informáticos para reducir el riesgo de brechas de información. Se deberán al menos realizar las siguientes verificaciones:

- *Parcheo y actualización de software*
- *Cifrado fuerte de datos para datos sensibles*
- *Mejora, renovación y actualización de dispositivos (por ejemplo, equipos que ya no cuentan con soporte por parte del proveedor)*
- *Reforzar políticas de uso de dispositivos personales (por ejemplo, requerir que se use un servicio de Red Privada Virtual o VPN y software antivirus)*
- *Uso de contraseñas fuertes y autenticación multi factor*
- *Capacitación del personal en mejores prácticas de seguridad informática y estrategias para reducir riesgos por ataques de ingeniería social.*

5. Doble factor de autenticación, mediante un código obtenido por una aplicación, correo electrónico y/o mensaje SMS que valide la identidad del usuario de la PDN.

6. Los sistemas en donde se aloja la PDN cuentan con al menos cuatro capas de defensa las cuales se mencionan a continuación: Sistema Operativo, Aplicaciones, Segmento de red y red perimetral:

***Sistema Operativo**: es el software principal de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software. La seguridad en la capa del Sistema Operativo significa que se cuenta con estrategias a nivel del Sistema Operativo instalado en los equipos de cómputo que procesan los datos personales. Por ejemplo:*

- *Aplicación periódica de actualizaciones del sistema operativo.*
- *Disponer de software antivirus actualizado.*
- *Escrutinio de trafico de red entrante y saliente a través de un firewall.*
- *Creación de cuentas seguras con los permisos estrictamente necesarios.*
- *Implementación de cifrado a nivel de dispositivos de almacenamiento o sistema de archivos.*

***Aplicaciones**: Se refiere a la aplicación de actualizaciones de seguridad de las aplicaciones que procesan datos personales.*

***Segmento de red**: Se refiere a que los datos personales se encuentran resguardados en una subred de la red de computadoras de la SESNA, a la que solo se puede acceder con permisos especiales. Los usuarios comunes de la red de la SESNA se encuentran en una subred que no les permite tener acceso a los recursos de cómputo que procesan los datos personales.*

***Red perimetral**: La red perimetral o DMZ (zona desmilitarizada) se refiere a una subred de la SESNA, donde se encuentran los equipos de cómputo que pueden ser accedidos desde fuera de la red de la SESNA (los equipos de la DMZ no deben conectarse directamente con la red interna).Esto permite que los equipos de la DMZ puedan dar servicios a la red externa, a la vez que protegen la red interna*

en el caso de que un intruso o atacante comprometa la seguridad de los equipos situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

7. Política de contraseñas seguras mediante el uso de contraseñas largas, con combinaciones complejas de caracteres que incluyan mayúsculas, minúsculas, números y signos de puntuación o símbolos, considerando sean cambiadas cada 90 días.

8. Los responsables deberán atender siempre las recomendaciones emitidas por la USTPDN respecto a los protocolos, niveles y medidas de seguridad para lograr la interoperabilidad con la PDN. De no atenderse, la USTPDN se reserva el derecho a realizar la conexión de sus sistemas con la PDN." (Sic)

Ahora bien, en la atención al requerimiento de información adicional, la SESNA manifestó lo siguiente:

*"**15.** Los sistemas informáticos donde se aloja la PDN cuentan con al menos cuatro capas de defensa las cuales se mencionan a continuación:*

Capa 1. Sistema Operativo

El sistema operativo es el software principal de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software. En el contexto de la PDN, la seguridad en la capa del Sistema Operativo refiere a que se cuenta con estrategias a nivel del Sistema Operativo instalado en los equipos de cómputo que procesan los datos personales. Por ejemplo:

- *Aplicación periódica de actualizaciones del sistema operativo*
- *Disponer de software antivirus actualizado*
- *Escrutinio de tráfico de red entrante y saliente a través de un firewall*
- *Creación de cuentas seguras con los permisos estrictamente necesarios*
- *Implementación de cifrado a nivel de dispositivos de almacenamiento o sistema de archivos*

Capa 2. Aplicaciones

Se refiere a la aplicación de actualizaciones de seguridad de las aplicaciones que procesan datos personales y a la implementación de cifrado de comunicaciones (por ejemplo, a través de certificados SSL).

Capa 3. Segmento de red

Se refiere a que los datos personales se encuentran resguardados en una subred de la red de computadoras de la SESNA, a la que solo se puede acceder con permisos especiales. Los usuarios comunes de la red de la SESNA se encuentran en una subred que no les permite tener acceso a los recursos de cómputo que procesan los datos personales.

Capa 4. Red perimetral

La red perimetral o DMZ (zona desmilitarizada) se refiere a una subred de la SESNA, donde se encuentran los equipos de cómputo que pueden ser accedidos desde fuera de la red de la SESNA (los equipos de la DMZ no deben conectarse directamente con la red interna).

Esto permite que los equipos de la DMZ puedan dar servicios a la red externa, a la vez que protegen la red interna en el caso de que un intruso o atacante comprometa la seguridad de los equipos situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

Otras medidas de seguridad
Adicionalmente, como medidas de seguridad físicas y administrativas, se cuenta con acceso restringido a las instalaciones de la Secretaría, además de un servicio continuo de orientación, mantenimiento y soporte técnico por parte de la Unidad de Servicios Tecnológicos y Plataforma Digital Nacional."

Al respecto, la SESNA, manifestó que las medidas de protección para no correr riesgos, respecto a la protección de datos personales es a través de la definición del protocolo REST para la interconexión de los sistemas que integran la plataforma, medidas de seguridad técnicas que se consideran suficientes por la naturaleza de los datos que serán tratados, adicionalmente, se hace la observación de que la plataforma hereda medidas de seguridad de los sistemas con los que se comunica, por lo que se debe incluir un análisis que identifique si la comunicación de la información representa un riesgo para la plataforma. Si bien, se entregaron documentos que indican parámetros y mínimos requeridos para la interconexión, no se puede dar por sentado que los documentos se refieren específicamente a medidas de seguridad administrativas, es así que se determina que, el sujeto obligado omitió las medidas de seguridad administrativas y físicas que se deben considerar según lo dispuesto por el artículo 15, fracción XIII.

Derivado de lo anterior, es posible apreciar que la SESNA únicamente manifestó que cuenta con medidas de seguridad técnicas implementadas a partir de la definición del protocolo de comunicación entre Sistemas, la cual es una medida de seguridad técnica aplicable al tratamiento de datos personales, sin embargo, el sujeto obligado no proporcionó información suficiente para valorar que dicha medida de seguridad es suficiente, ya que, no hay evidencias que indiquen que no hay riesgos por el intercambio de información a partir del protocolo de comunicación.

En este sentido, es posible advertir que la SESNA, no ha realizado un debido análisis de riesgos que le permita identificar las medidas de seguridad necesarias a implementar ya que, de acuerdo con la descripción, existen amenazas intrínsecas que no son reportadas ni mucho menos analizadas, por lo que se espera que se incluyan reportes que pongan en evidencia la seguridad de las comunicaciones entre sistemas y finalmente, la descripción de las medidas de seguridad administrativas y físicas que se identifiquen y acrediten respecto de la propia plataforma.

Asimismo, si bien la SESNA remitió su Documento de Seguridad, también se advierte que, en el mismos no se advierte el inventario de datos personales ni de los sistemas con los sistemas 1, 2, 3, 4, 5 y 6 de la PDN interactúan; ni tampoco se realizó referencia específica a su actualización en términos del artículo 36 de la Ley General.

Al respecto, la SESNA está obligada a realizar al menos las siguientes acciones interrelacionadas:

- Crear políticas internas para la gestión y tratamiento de los datos personales, tomando en cuenta el contexto en el que se lleva a cabo el tratamiento a través de la PDN y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.
- Definir las funciones y obligaciones de todo el personal involucrado, desde la SESNA hasta la empresa contratada para el desarrollo de la plataforma, en el tratamiento de datos personales.
- Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, el hardware, software, personal del responsable.
- Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización de la SESNA.
- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales a través de la SESNA.
- Monitorear y revisar periódicamente las medidas de seguridad que determine implementar, así como las amenazas y vulneraciones a las que están sujetos los datos personales que se tratarán a través de la propia PDN.
- 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 que se pretende con la puesta en operación de la aplicación electrónica.

Por lo antes dicho, y atendiendo a lo manifestado en las constancias del presente expediente, se advierte que la SESNA brinda evidencia de forma parcial sobre el cumplimiento con la adopción de medidas de seguridad de carácter administrativo, físico y técnico en el diseño y operación de la PDN.

3. Deber de confidencialidad

El artículo 42 de la Ley General dispone lo siguiente:

> *"**Artículo 42.** El 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.*
>
> *Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública."*

A su vez, el artículo 71 de los Lineamientos Generales señala lo siguiente:

> *"**Deber de confidencialidad***

> ***Artículo 71.*** *El 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."*

De las disposiciones anteriores, se desprende que el responsable está obligado a guardar reserva y sigilo durante todo el tratamiento de los datos personales.

En virtud de lo anterior, la SESNA refirió que:

> *"Uno de los objetivos de la PDN es la rendición de cuentas y generar inteligencia por lo que garantizar el mayor grado de accesibilidad se considera como un elemento positivo. Sin embargo, se implementarán todas las medidas de seguridad necesarias para salvaguardar la secrecia de la información clasificada por el Comité Coordinador como confidencial y asegurar que únicamente las autoridades con facultades legales puedan acceder a estos datos.*
> *[...]*
>
> *Es fundamental mencionar que el acceso a los datos reservados se realizará con base en los permisos que el Comité Coordinador del SNA y con base en las atribuciones que la legislación aplicable confiere a aquellos que pueden consultar los datos reservados." (Sic)*

Asimismo, la SESNA refirió que actualmente la PDN dispone únicamente de información pública, permitiendo la consulta de información no reservada de manera pública y anónima, por lo cual, se cuenta con un registro con fines estadísticos que permite identificar únicamente búsquedas frecuentes y otras métricas de uso a través de la tecnología conocida como Google Analytics.

Al respecto, cabe mencionar que las Bases para el funcionamiento de la PDN, establecen lo siguiente:

> ***"Artículo 17.*** *Los diferentes niveles de acceso a la Plataforma se definirán conforme a los derechos, atribuciones y competencias de cada usuario, conforme a la normativa aplicable a cada uno de los sistemas.*
> ***Artículo 18.*** *La Secretaría Ejecutiva elaborará y publicará un catálogo de perfiles, en el cual se establezcan las facultades, obligaciones, y/o atribuciones que les sean aplicables a cada uno de los usuarios de manera genérica.*
> ***Artículo 19.*** *Para el acceso restringido de la información, la Secretaría Ejecutiva establecerá los mecanismos de seguridad necesarios que garanticen la confidencialidad, integridad y disponibilidad de la información.*
> ***Artículo 20.*** *La colaboración para el adecuado funcionamiento de la Plataforma será obligatoria para todos los entes públicos a nivel federal, estatal y municipal, de conformidad con lo establecido en las presentes bases y la legislación aplicable.*
> ***Artículo 21.*** *Para aquellos datos que sean de dominio público, la Plataforma seguirá las disposiciones en materia de transparencia, acceso a la información, datos abiertos y protección de datos personales aplicables.*

> ***Artículo 22.*** *La Secretaría Ejecutiva, propondrá y diseñará los talleres de aprendizaje en el uso de la Plataforma, y será responsable de brindar capacitación técnica y de operación de la Plataforma a los usuarios, proveedores, concentradores y encargados."*

De lo anterior, es posible advertir que en principio la información contenida actualmente en la PDN es pública, por lo cual no cuenta en principio con el carácter de confidencial.

No obstante, respecto de aquella información que pudiera tener el carácter de reservada o confidencial, en términos de la Ley General de Transparencia y Acceso a la información Pública, la SESNA manifestó que se encuentran en elaboración el documento con el Catálogo de perfiles que establecerá quiénes son los usuarios que podrán acceder a la información reservada, conforme a la normativa aplicable- por lo que en tanto dicho documento no sea emitido, la PDN no permitirá la consulta y el intercambio de los datos reservados.

De lo anterior es posible advertir que la SESNA cumple de manera parcial con el deber de confidencial pues, si bien refiere en la normatividad que se implementaran los mecanismos necesarios para garantizar la confidencialidad de la información, no se cuenta con evidencia que permita dilucidar que ha establecido este tipo de controles o mecanismos que permitan acreditar el cumplimiento de su obligación para garantizar la confidencialidad de los datos personales que son tratados a través de la PDN.

Por lo tanto, en su carácter de sujeto obligado, la SESNA deberá implementar algún tipo de control o mecanismo que tenga como propósito que todas las personas que intervengan en el tratamiento de los datos personales tratados a través de la PDN guarden confidencialidad respecto de tales datos personales, como podrían ser:

- Elaboración de cláusulas contractuales que refieran la obligación de guardar la confidencialidad respecto de los datos personales que, con motivo de las funciones que realiza, conozca.
- Elaboración cartas compromiso dirigidas a todo el universo de usuarios, es decir, a cualquiera persona que por cualquier motivo participe en el tratamiento de datos personales que conformarán los sistemas de la PDN; en las que se refiera que la obligación de guardar confidencialidad respecto de los datos personales, con motivo de las funciones que se realizaran a través de plataforma.
- En general la elaboración de cualquier documento o instrumento que permita acreditar que el responsable cuenta con mecanismos que garanticen la confidencialidad de los datos personales que recaba.

4. Derechos ARCO y portabilidad de datos personales

Los artículos 43, 44, 45, 46, 47, 49, 50, 51, 52, 53, 54, 55 y 86 de la Ley General, los artículos 73, 76, 77, 78, 79, 80, 81, 91, 92, 93, 94 y 95 de los Lineamientos generales, de los cuales se advierte que los derechos ARCO son prerrogativas que tiene toda persona física para:

- Acceder a los datos personales y conocer la información relacionada con las condiciones y generalidades de su tratamiento.
- Rectificar sus datos personales cuando resulten ser inexactos, incompletos o no se encuentren actualizados.
- Cancelar sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.
- Oponerse al tratamiento de sus datos personales cuando aun siendo lícito el tratamiento, el mismo deba cesar para evitar que su persistencia cause un daño o perjuicio al titular y los datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

En este sentido, la solicitud para el ejercicio de los derechos ARCO debe señalar lo siguiente:

- El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones.
- Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.
- De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud.
- La descripción clara y precisa de los datos personales respecto de los que el titular busca ejercer alguno de los derechos ARCO.
- La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular.
- Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.
- Tratándose del ejercicio del derecho de acceso, deberá contener el señalamiento de la modalidad en la que el titular prefiere que sus datos personales se reproduzcan.

Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante, conforme las siguientes reglas:

- El titular deberá acreditar su identidad a través de los medios previstos en el artículo 76 de los Lineamientos generales. Por su parte, su representante deberá acreditar su identidad y la personalidad con la que actúa conforme a los medios enlistados en el artículo 77 de los Lineamientos generales.
- En el caso del ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación.
- Para la acreditación de la identidad de un menor y la representación de los padres que ejercen la patria potestad, de una persona distinta a los padres que ejercen la patria potestad o del tutor se deberán observar las reglas y medios previstos en los artículos 78, 79 y 80 de los Lineamientos generales.
- Cuando el titular sea una persona en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, además de acreditar la identidad de la persona, su representante deberá acreditar su identidad y representación conforme a los medios previstos por el artículo 81 de los Lineamientos generales.

Es por ello, que el responsable se encuentra obligado a establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO de los datos personales utilizados, bajo las siguientes condiciones:

- Los derechos ARCO se pueden ejercer en cualquier momento, donde el ejercicio de cualquiera de ellos no es requisito previo, ni impide el ejercicio de otro.
- Procurar que las personas con algún tipo de discapacidad o grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.
- La prohibición de imponer al titular mayores requisitos en las solicitudes para el ejercicio de los derechos ARCO que las señaladas en el artículo 52 de la Ley General y 83 de los Lineamientos generales.
- La prohibición de aumentar los plazos previstos en el artículo 51 de la Ley General para la atención y respuesta de solicitudes para el ejercicio de los derechos ARCO, los cuales se traducen en 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para que el responsable determine la procedencia o improcedencia del derecho de que se trate, el cual podrá ampliarse por una sola vez hasta por 10 días hábiles. En caso de que resulte procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días hábiles, contados a partir del día siguiente en que se haya notificado la respuesta al titular.
- El ejercicio del derecho de acceso es gratuito. Los cobros solo podrán realizarse cuando se quiera recuperar los costos de reproducción, certificación o envío.

De esta manera, la obligación de acceso a los datos personales se dará por cumplida cuando el responsable ponga a disposición del titular, previa acreditación de su identidad y, en su caso, la identidad y personalidad de su representante, los datos personales a través de los medios previstos en el artículo 92 de los Lineamientos Generales.

Asimismo, la obligación de rectificar los datos personales se dará por cumplida cuando el responsable notifique al titular, previa acreditación de su identidad y, en su caso, la identidad y personalidad de su representante, una constancia que acredite la corrección solicitada. Para ello deberá considerar, al menos, los requisitos previstos por el artículo 93 de los Lineamientos generales.

Por su parte, la obligación de cancelar los datos personales se dará por cumplida cuando el responsable notifique al titular, previa acreditación de su identidad y, en su caso la identidad y personalidad de su representante, una constancia que cumpla con los requisitos y formalidades previstas en el artículo 94 de los Lineamientos generales.

Mientras que la obligación de cesar el tratamiento de los datos personales se dará por cumplida cuando el responsable notifique al titular, previa acreditación de su identidad y, en su caso, la identidad y personalidad de su representante, una constancia que señale dicha situación.

Finalmente, el responsable podrá determinar la improcedencia del ejercicio de los derechos ARCO cuando se actualice alguna de las siguientes razones:

- El titular o su representante no estén debidamente acreditados.
- Los datos personales no se encuentren en posesión del responsable.
- Exista un impedimento legal.
- Se lesionen los derechos de un tercero.
- Se obstaculicen actuaciones judiciales o administrativas.
- Exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos.
- La cancelación u oposición haya sido previamente realizada.
- El responsable no sea competente.
- Los datos personales sean necesarios para proteger intereses jurídicamente tutelados del titular.
- Los datos personales sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular.
- En función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano.

- Los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del responsable hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

Sobre el particular, la SESNA manifestó en el Documento de Seguridad, siguiente:

> *"[…]*
>
> *Para todos los sistemas de tratamiento de datos personales*
> *El acceso, rectificación, cancelación y oposición de los datos personales se deberá solicitar a los Encargados, ya que son ellos los responsables de la administración de las bases de datos y sistemas donde se almacenan los datos personales que obtienen.*
> *[…]" (Sic)*

Ahora bien, como ya se ha señalado en el presente análisis, los datos personales que serán parte de los sistemas que conforman la PDN serán obtenidos por la SESNA de manera indirecta, toda vez que los entes públicos, con atribuciones en la materia, serán los encargados de recabar los datos personales de los titulares que formarán parte de los sistemas de la PDN, además serán los que den almacenamiento a dichos datos. En este sentido, al obtener directamente los datos personales, los entes públicos son los responsables ante quienes los titulares podrán solicitar el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen en términos de lo dispuesto en el artículo 43 de la Ley General a efecto de que se le pueda dar trámite y respuesta en términos del artículo 48 de la citada ley.

Por lo anterior, si bien, la SESNA no estará obligada a realizar la recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO de los titulares de los datos personales que formarán parte de la información contenida en los sistemas que integran la PDN, tomando en consideración las manifestaciones realizadas en el principio de información respecto de los datos personales obtenidos a través del registro de usuarios con privilegios, es preciso señalar que, una vez que se implemente esta funcionalidad para dicho proceso de registro, la SESNA estará obligada a adoptar los mecanismos y medios que estime pertinentes orientados para garantizar el ejercicio de los derechos ARCO de los titulares que realicen dicho registro de usuarios con privilegios, informados mediante el respetivo aviso de privacidad, de conformidad con las disposiciones citadas anteriormente de la Ley General y los Lineamientos generales, las cuales, de manera general, se traducen en lo siguiente:

- Los derechos ARCO se pueden ejercer en cualquier momento, donde el ejercicio de cualquiera de ellos no es requisito previo, ni impide el ejercicio de otro.
- Las únicas personas acreditadas para ejercer derechos ARCO son el titular o su representante, menores de edad o personas que se encuentren en estado de interdicción o

incapacidad declarada en ley con su debida representación conforme a las reglas civiles que resulten aplicables y personas vinculadas a fallecidos.

- La prohibición de imponer mayores requisitos en las solicitudes para el ejercicio de los derechos ARCO que las señaladas en el artículo 52 de la Ley General y 83 de los Lineamientos Generales.
- La prohibición de aumentar los plazos previstos en el artículo 51 de la Ley General para la atención y respuesta de solicitudes para el ejercicio de los derechos ARCO, los cuales se traducen en 20 días hábiles, contados a partir del día siguiente a la recepción de la solicitud, para que la SESNA determine la procedencia o improcedencia del derecho de que se trate, el cual podrá ampliarse por una sola vez hasta por 10 días hábiles. En caso de que resulte procedente el ejercicio de los derechos ARCO, la SESNA deberá hacerlo efectivo en un plazo que no podrá exceder de 15 días hábiles, contados a partir del día siguiente en que se haya notificado la respuesta al titular.
- Procurar que las personas con algún tipo de discapacidad o grupos vulnerables, puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.
- La prohibición de cobrar costos a los representantes de los niños y adolescentes por el ejercicio de sus derechos ARCO, más allá de aquellos relacionados con la reproducción, certificación y envío de datos personales.

Asimismo, la SESNA estará obligado a garantizar el derecho a la portabilidad de conformidad con el artículo 57 de la Ley General en caso de que la PDN genere un formato estructurado y comúnmente utilizado a que se refiere el artículo 6 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales,[18] es decir, que se trate de un formato electrónico accesible y legible por medios automatizados de tal forma que éstos puedan identificar, reconocer, extraer, explotar o realizar cualquier otra operación con datos personales específicos; el formato permita la reutilización y/o aprovechamiento de los datos personales y el formato sea interoperable con otros sistemas informáticos de conformidad con lo dispuesto en el artículo 2, fracción I de los aludidos Lineamientos. Lo anterior, sin menoscabo de la actualización de las causales de improcedencia previstas en el artículo 55 de la Ley General.

Al respecto, la SESNA no realizó manifestación alguna en la evaluación de impacto de la PDN, ni en la respuesta al requerimiento de información adicional sobre la posibilidad de ejercer este derecho con respecto al tratamiento de datos personales que se llevará a cabo mediante la PDN.

[18] DOF. (2019). Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. Consultado el 10/12/2019. Dirección URL: http://www.dof.gob.mx/nota_detalle.php?codigo=5612847&fecha=12/02/2018 consultados por última vez el 18/05/2021

Derivado de lo anterior, este Instituto determina que, hasta el momento de la presentación de la evaluación de impacto en la protección de datos personales que nos ocupa, SESNA no tiene previsto la posibilidad de ejercer este derecho con respecto al tratamiento de datos personales que se llevará a cabo mediante la PDN.

5. Encargado

Los artículos 3, fracciones VI y XV, 58, 59, 60, 61, 62, 63, 64 y 71 de la Ley General, 108, 109, 110, 111 y 112 de los Lineamientos generales, de los que se advierte que el encargado es una persona física o moral, de carácter público o privado, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales a nombre y por cuenta de éste.

Es decir, el encargado es un prestador de servicios que realiza actividades de tratamiento de datos personales a nombre y por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que lo vincula con el mismo y delimita el ámbito de su actuación en la prestación de un servicio.

En ese sentido, la figura del encargado debe cumplir con cada una de las siguientes características:

- . Puede ser una persona física o moral del ámbito público o privado.
- Ser ajeno a la organización del responsable, es decir, los trabajadores que forman parte de la estructura del responsable no tienen la calidad de encargados.
- Puede tratar los datos personales solo o en conjunto con otras personas.
- Se vincula con el responsable a través de una relación jurídica que delimita el ámbito de su actuación.
- No ostenta poder de decisión sobre el tratamiento de los datos personales que efectúe, sino que en virtud de la relación jurídica que lo vincula con el responsable se limita a tratarlos a nombre y por cuenta de este último, siguiendo expresamente sus instrucciones.

En otras palabras, el encargado actualiza una especie de delegación de funciones en el tratamiento de los datos personales que lleve a cabo, acotando su actuación a las instrucciones dadas por el responsable y sin ostentar poder alguno de decisión sobre el alcance y contenido del tratamiento.

En este sentido, el responsable está obligado a formalizar con el encargado la prestación de sus servicios a través de la suscripción de un contrato o cualquier otro instrumento jurídico de conformidad con la normatividad que le resulte aplicable, considerando, al menos, las siguientes cláusulas relacionadas con los servicios contratados:

- Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.
- Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.
- Implementar las medidas de seguridad conforme a la Ley General, los Lineamientos generales y demás instrumentos jurídicos aplicables.
- Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.
- Guardar confidencialidad respecto de los datos personales tratados.
- Suprimir o devolver los datos personales, objeto de tratamiento, una vez cumplida la prestación de servicios con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
- Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine o la comunicación derive de una subcontratación o por mandato expreso de la autoridad competente.
- Permitir al Instituto o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de los datos personales.
- Colaborar con el Instituto en las investigaciones previas y verificaciones que lleve a cabo, en términos de lo dispuesto en la Ley General, los Lineamientos generales y demás normatividad aplicable.
- Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.

Asimismo, el responsable está obligado a autorizar expresamente la subcontratación de servicios que involucren el tratamiento de datos personales, ya sea en el propio contrato o instrumento jurídico que suscriba con el prestador de servicios o encargado, o bien, de manera previa a la contratación.

Cuando la subcontratación de servicios sea autorizada por el responsable, el encargado está obligado a formalizar ésta a través de la suscripción de un contrato o cualquier otro instrumento jurídico que determine el encargado, el cual debe contener, al menos, las cláusulas previstas para la formalización de la prestación de servicios entre el responsable y el encargado.

En caso de que el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre los fines, medios y demás cuestiones relacionadas con el tratamiento de datos personales instruido por el responsable, asumirá el carácter de responsable conforme a la legislación que le resulte aplicable en función de que su naturaleza sea pública o privada.

El responsable está obligado, en su caso, a contratar o adherirse a aquellos servicios de cómputo en la nube y otras materias, entendidos como modelos 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, que garanticen políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la Ley General, los Lineamientos Generales y demás normatividad derivada.

Los proveedores de servicios de cómputo en la nube y otras materias tienen la calidad de encargados, por lo cual, si el responsable tiene la posibilidad de convenir con el proveedor las condiciones y términos de este tipo de servicios a través de la suscripción de un contrato o instrumento jurídico específico, éste debe prever, al menos, las cláusulas generales señaladas en los artículos 59 de la Ley General y 109 de los Lineamientos generales, obligación que no exime al responsable de observar lo siguiente:

- Que el servicio de cómputo en la nube o de otras materias cumpla, al menos, con:
  - Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley General, los Lineamientos generales y demás normativa aplicable.
  - Transparentar las subcontrataciones que involucren los datos personales sobre los que se preste el servicio.
  - Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de los datos personales sobre los que se preste el servicio.
  - Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.
- Que los servicios de cómputo en la nube o de otras materias cuenten con mecanismos, al menos, para:
  - Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que se preste.
  - Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se preste el servicio.
  - Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio.
  - Garantizar la supresión de los datos personales una vez que hubiere concluido el servicio prestado al responsable y que este último haya podido recuperarlos.
  - Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente informar sobre tal situación al responsable.

En caso contrario, el responsable sólo está obligado a observar las reglas previstas en los artículos 59 de la Ley General y 109 de los Lineamientos generales.

Al respecto, la SESNA no realizó manifestación alguna en la evaluación de impacto de la PDN, ni en la respuesta al requerimiento de información adicional sobre la contratación o prestación de servicios por un Encargado.

Derivado de lo anterior, este Instituto determina que, hasta el momento de la presentación de la evaluación de impacto en la protección de datos personales que nos ocupa, la SESNA no tiene previsto contratar servicios de terceros que implicarían un tratamiento de datos personales a través de la PDN.

Por lo anterior, en caso de que la SESNA decidiera contratar los servicios de terceros para el tratamiento de los datos personales que se llevará a través de la PDN estaría obligado a cumplir con lo dispuesto en los artículos 58, 59, 60, 61, 62, 63, 64 y 71 de la Ley General y 108, 109, 110, 111 y 112 de los Lineamientos generales.

6. Transferencias

Los artículos 3, fracción XXXII, 65, 66, 67, 68, 69 y 70 de la Ley General, 113, 114, 115 y 116 de los Lineamientos generales, que disponen que toda comunicación de datos personales, sea nacional o internacional, realizada a persona distinta del responsable, encargado y titular se denomina transferencia.

En este sentido, toda transferencia de datos personales que se efectúe debe estar autorizada previamente por el titular, salvo que se actualice alguna de las siguientes excepciones:

- Cuando la transferencia de los datos personales esté prevista en una ley, convenio o tratado internacional suscrito y ratificado por México.
- Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
- Cuando la transferencia de los datos personales sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia.
- Cuando la transferencia de los datos personales sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última.

- Cuando la transferencia de los datos personales sea necesaria para la prevención, diagnóstico médico, prestación de asistencia sanitaria, tratamiento médico o gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados.
- Cuando la transferencia de los datos personales sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.
- Cuando la transferencia de los datos personales sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.
- Cuando el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales.
- Cuando la transferencia de datos personales sea necesaria por razones de seguridad nacional.

Cabe señalar, que el hecho de que el responsable no esté obligado a requerir el consentimiento del titular para la transferencia de sus datos personales, de ninguna manera, deberá entenderse que esta excepción se extienda o resulte aplicable a la observancia de las demás obligaciones previstas en la Ley General, los Lineamientos generales y demás disposiciones aplicables.

Por regla general, la autorización del titular para la transferencia de sus datos personales debe ser en la modalidad tácita, salvo que una disposición legal exija al responsable recabar el consentimiento expreso del titular. En aquellos casos donde se requiera el consentimiento expreso del titular, el responsable está obligado a establecer cualquier medio que le permita obtener dicho consentimiento de manera previa a la transferencia de los datos personales, siempre y cuando el medio habilitado sea de fácil acceso y con la mayor cobertura posible, considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común con éstos.

Asimismo, el responsable transferente de los datos personales está obligado a:

- Informar en su aviso de privacidad los destinatarios de los datos personales y las finalidades que motivaron la comunicación de los mismos.
- Limitar el tratamiento de los datos personales transferidos a las finalidades que originaron la misma.
- Comunicar su aviso de privacidad al receptor o destinatario de los datos personales.
- Formalizar la transferencia de datos personales mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, que le permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes, salvo que se actualice alguna de las siguientes excepciones:

- Cuando la transferencia de datos personales sea nacional y se realice entre responsables en cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos.
- Cuando la transferencia de datos personales sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el transferente y el receptor sean homólogas, o bien, las finalidades que motivan la transferencia de datos personales sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.

Cuando se trate de una transferencia nacional de datos personales, además de las reglas generales señaladas anteriormente, el receptor o destinatario de los datos personales:

- Asume el carácter de responsable conforme a la legislación que en esta materia le resulte aplicable, atendiendo a su naturaleza jurídica, pública o privada.
- Está obligado a tratar los datos personales conforme a dicha legislación y a lo convenido en el aviso de privacidad que le será comunicado por el responsable.
- Debe garantizar la confidencialidad de los datos personales.
- Está obligado a tratar los datos personales para las finalidades que motivaron su transferencia atendiendo a lo convenido en el aviso de privacidad del responsable transferente.

Si se trata de una transferencia internacional de datos personales, además de las reglas generales señaladas anteriormente, el responsable sólo podrá transferir datos personales fuera del territorio nacional cuando el receptor o destinatario se obligue a proteger los datos personales conforme a obligaciones similares o equiparables a las previstas en la Ley General, los Lineamientos generales y demás normatividad mexicana aplicable en la materia, así como a los términos establecidos en el aviso de privacidad que le será comunicado por el responsable transferente.

Sobre el particular, la SESNA señaló lo siguiente:

> *"II.6 Transferencias*
> *Tomando en cuenta que por "transferencia" se debe entender toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado,13 se manifiesta que la información contenida en el S1 es susceptible de ser transferida a las diversas autoridades de los tres órdenes de gobierno, competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción, entre las que se encuentran el Ministerio Público, órganos jurisdiccionales como el Tribunal Federal de Justicia Administrativa y sus homólogos en las entidades federativas, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras a las que alude la LGRA, como la Secretaría de la Función Pública en el Poder Ejecutivo*

Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos.
[...]
III.6 Transferencias
No aplica.
Lo anterior, en virtud de que el S2 es solo un sistema de consulta para las diversas autoridades de los tres órdenes de gobierno, competentes en la prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos.
[...]
IV.6 Transferencias
No aplica.
En virtud de que el S3 es solo un sistema de consulta para los Entes públicos del Estado mexicano que pretendan realizar un nombramiento, designación o contratación.
[...]
V.6 Transferencias
No aplica.
Lo anterior, en virtud de que el S6 es solo un sistema de consulta tanto para Entes públicos como ciudadanía en general, para facilitar la prevención, detección, investigación y sanción de faltas administrativas y hechos de corrupción, así como de control y fiscalización de recursos públicos
[...]". (Sic)

Derivado de lo anterior, la SESNA manifestó que la información contenida en el S1, es decir, lo respectivo a las declaraciones patrimoniales y de intereses, así como la constancia de presentación de declaración fiscal, es susceptible de ser transferida a las diversas autoridades de los tres órdenes de gobierno, competentes en la prevención, investigación y sanción de faltas administrativas y hechos de corrupción, entre las que se encuentran el Ministerio Público, órganos jurisdiccionales como el Tribunal Federal de Justicia Administrativa y sus homólogos en las entidades federativas, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras a las que alude la Ley General de Responsabilidades, como la Secretaría de la Función Pública en el Poder Ejecutivo Federal y sus homólogos en las entidades federativas, así como los Órganos Internos de Control de los Entes públicos.

Por lo que refiere al resto de los sistemas que conformarán la PDN, se advierte que no se llevará a cabo transferencias.

Al respecto, el artículo 28 de la Ley General de Responsabilidades establece que la información relacionada con las declaraciones de situación patrimonial y de intereses, podrá ser solicitada y utilizada por el Ministerio Público, los Tribunales o las autoridades judiciales en el ejercicio de sus respectivas atribuciones, el Servidor Público interesado o bien, cuando las Autoridades investigadoras, substanciadoras o resolutoras lo requieran con motivo de la investigación o la resolución de procedimientos de responsabilidades administrativas.

En este sentido el artículo 42 de las Bases para el funcionamiento de la PDN, dispone que la SESNA deberá establecer los mecanismos para que la información de dicho sistema **sea solicitada y utilizada** de acuerdo con las necesidades de las autoridades competentes antes mencionadas, en el ejercicio de sus respectivas atribuciones y de conformidad con la normativa aplicable, previa aprobación del Comité Coordinador.

Por lo anterior, y por lo que hace al Sistema 1 relacionado con las declaraciones de situación patrimonial y de intereses; las disposiciones legales antes mencionadas determinan que el Ministerio Público, Tribunales o autoridades judiciales, servidores públicos, autoridades investigadoras, sustanciadoras o resolutoras en el ejercicio de sus respectivas atribuciones y de conformidad con la normativa aplicable, previa aprobación del Comité Coordinador podrán solicitar la información relacionada con las declaraciones de situación patrimonial y de intereses a fin de ser utilizadas con respecto a sus respectivas atribuciones.

Al respecto la SESNA determina que, para tal solicitud y utilización, se deberán establecer mecanismos que permitan la posibilidad de transferir dicha información a las autoridades competentes, antes referidas, con el con el objetivo de ser utilizadas para investigar y sancionar posibles faltas administrativas o delitos de corrupción.

De lo anterior, se identifica que, para cumplir con la solicitud de dichas autoridades competentes y en su caso, puedan ser utilizadas en el ejercicio de sus respectivas atribuciones, la SESNA, como administradora del funcionamiento de esta plataforma, sea a través de los mecanismos que permitirán a estas autoridades como usuarios de la PDN, un acceso a dicha información, lo cual actualizará una comunicación a estas autoridades de las declaraciones patrimoniales y de intereses.

De esta manera, se advierte que se actualizarían transferencias de datos personales contenidos en el S1, Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal, entendida como toda comunicación de datos personales, dentro o fuera de territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado, de conformidad con lo establecido en el artículo 3, fracción XXXII, de la Ley General.

En este sentido, al actualizarse una transferencia de datos personales respecto del tratamiento realizado a través de la PDN, la SESNA en cumplimiento con el régimen establecido en la Ley General respecto del tratamiento de transferencias, por lo que hace al artículo 65 de la Ley General, donde se contempla que toda transferencia de datos personales se encuentra sujeta al consentimiento del titular, salvo que se actualice alguna de las excepciones señaladas en la Ley, se hace propio lo establecido en el principio de consentimiento previamente señalado.

Cabe señalar que por lo que hace a lo establecido en el artículo 66 de la Ley General, es posible advertir que las transferencias de datos personales contenidos en el S1, Sistema de evolución patrimonial, de declaración de intereses y constancia de presentación de declaración fiscal, se realizarán entre la SESNA y las autoridades competentes, previamente señaladas, en virtud del cumplimiento de lo establecido en la Ley General de Responsabilidades, así como en las Bases para el funcionamiento de la PDN, por lo cual, no será necesario formalizarse mediante la a suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, en términos del artículo 66, fracción I.

Ahora bien, en términos del artículo 35 de los Lineamientos Generales, la SESNA, deberá informar mediante su aviso de privacidad integral, la transferencia que efectúa, en virtud de recomendación señalada en el principio de información.

VIII. Conclusiones y recomendaciones.

De las consideraciones anteriores, se concluye que los controles y medidas que la SESNA adoptará para gestionar los riesgos asociados al tratamiento de datos personales que conllevará la puesta en operación de la PDN; así como los mecanismos o procedimientos que implementará para que el tratamiento de los datos personales cumpla, desde el diseño y por defecto, con las obligaciones previstas en la Ley General, los Lineamientos generales y demás normatividad aplicable, son susceptibles de mejora. Por lo cual, se recomienda a la SESNA lo siguiente:

1. Identificación, análisis y gestión de los riesgos para la protección de los datos personales

- Fortalecer el análisis de riesgos a la PDN, llevando un nuevo ejercicio, de manera general y no sólo sobre los riesgos respecto del ámbito técnico y deberá contemplar al menos lo siguiente:
  - La identificación total de todos los actores involucrados y de los sistemas de tratamiento, como una exigencia derivada de lo previsto por el artículo 35, fracciones I y II, de la Ley General.
  - En términos de lo establecido en el punto que antecede, considerar a todos los actores involucrados que interoperan con la PDN (sistemas, subsistemas y componentes de entrada y salida), a fin de considerar en términos del artículo 32 de la Ley General, lo siguiente:
    a. El riesgo inherente a los datos personales tratados.
    b. La sensibilidad de los datos personales tratados.
    c. El desarrollo tecnológico.
    d. Las posibles consecuencias de una vulneración para los titulares.
    e. Las transferencias de datos personales que se realicen.

f. El número de titulares.
g. Las vulneraciones previas ocurridas en los sistemas de tratamiento.
h. 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.

Lo anterior, en la inteligencia que, por ejemplo, el registro de vulneraciones previas existentes en subsistemas con los que interactúa la PDN deben ser controlados a fin de evitar que se traduzcan en vulnerabilidades potenciales o reales.

- La identificación y descripción específica de los riesgos administrativos, físicos o tecnológicos; así como de los recursos humanos, técnicos, financieros, asociados;
- La ponderación cuantitativa y/o cualitativa de la probabilidad de que los riesgos identificados sucedan, así como su nivel de impacto en los titulares en lo que respecta al tratamiento de sus datos personales, y
- Las medidas y controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos detectados.
- Los demás elementos normativos a que hace referencia la Ley General y que se describen en el presente apartado, en particular, los elementos a que hacen referencia los artículos 31, 32 y 33 de la Ley General.

- Realizar un análisis de brecha, esto es, que el análisis se deberá realizar el comparativo entre las medidas de seguridad existentes y que son efectivas contra las medidas de seguridad que faltarían, cuyos resultados permitirían al responsable establecer las medidas de seguridad que podrían remplazar a uno o más controles implementados actualmente para la conexión entres sistemas de la PDN y sobre el funcionamiento de la misma.
- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales a través de la PDN así como de los sistemas fuentes de dónde se origina la información para consulta desde la plataforma, para lo cual se deberá tomar en cuenta los recursos destinados, el personal interno y externo de la SESNA y las fechas de compromiso para la implementación de dichas medidas nuevas o faltantes.
- Considerando las atribuciones de la SESNA en torno a la PDN, ante la actualización de una hipótesis normativa que dé lugar a la elaboración y presentación de una nueva Evaluación de impacto en la protección de datos personales, incorporar dentro de la misma la participación de las entidades, actores o sistemas vinculadas con la presentación a fin de que sea presentada una Evaluación de impacto en la protección de datos personales de carácter interinstitucional a que hace referencia el artículo 11 de las Disposiciones administrativas.

Por lo que este Instituto recomienda, realizar las siguientes acciones:

- Identificar la técnica de análisis de riesgos apropiada para la PDN de conformidad con los requerimientos normativos, administrativos y técnicos aplicable a la SESNA, tomando como punto de partida la referencia o exclusión expresa de la aplicabilidad del MAAGTICSI; a fin de que queden claramente comprendidas y justificadas las razones por las cuales se opta por una alternativa determinada, esto es así, puesto que el análisis de riesgo se llevó a cabo por BAA y no por el marco de MAAGTICSI, que eventualmente puede dar lugar a la implementación de análisis de riesgos en el marco de los estándares de la Organización Internacional de Estandarización en su serie 27000.
- Incorporar dentro del análisis de riesgos, análisis de brecha y plan de trabajo la identificación y acciones relacionadas con los sistemas y subsistemas con los que interactúa la PDN, a nivel federal, estatal y municipal, que le resultan exigibles a la SESNA en términos de sus atribuciones y en el marco de la implementación de su Sistema de Gestión.
- Realizar un nuevo análisis de riesgos a la PDN sobre los riesgos de conexión entre sistemas y sobre la plataforma misma, que contemple al menos lo siguiente:
    - La identificación y descripción especifica de los riesgos administrativos, físicos o tecnológicos[19];
    - La ponderación cuantitativa y/o cualitativa de la probabilidad de que los riesgos identificados sucedan, así como su nivel de impacto en los titulares en lo que respecta al tratamiento de sus datos personales, y
    - Las medidas y controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos detectados.
- Realizar un análisis de brecha, esto es, que el análisis se deberá realizar el comparativo entre las medidas de seguridad existentes y que son efectivas contra las medidas de seguridad que faltarían, cuyos resultados permitirían al responsable establecer las medidas de seguridad que podrían remplazar a uno o más controles implementados actualmente para la conexión entres sistemas de la PDN y sobre el funcionamiento de la misma.
- Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales a través de la PDN así como de los sistemas fuentes de dónde se origina la información para consulta desde la plataforma, para lo cual se deberá tomar en cuenta los recursos destinados, el personal interno y externo de la SESNA y las fechas de compromiso para la implementación de dichas medidas nuevas o faltantes.

2. Principios de protección de datos personales

- Se sugiere establecer algún mecanismo que le permita acreditar su obligación de respetar la expectativa razonable de privacidad del titular, estableciendo algún mecanismo especifico que

[19] Algunas herramientas de pruebas que se pueden utilizar son: Postman, Newnam, Apache Jmeter, SoapUI, Rest Assured, etc.

obligue a todos los usuarios de la PDN a privilegiar los intereses de las personas titulares, evitando que el tratamiento de los datos personales dé lugar a algún tipo de discriminación o trato injusto o arbitrario.

- Se recomienda a la SESNA que en caso de tratarse de sistemas cuyos datos sean generados o resguardados por autoridades que no formen parte del Comité Coordinador, respecto de los cuales se requerirá su consentimiento expreso para la inclusión mediante convenio que para tal efecto se celebre con la SESNA, se reconozca expresamente en dichos convenios que corresponderá a las autoridades correspondientes recabar el consentimiento de los titulares según sea el caso, para el tratamiento de sus datos personales conforme a las atribuciones y funciones conferidas por ministerio de ley, en términos de los artículos 20 de la Ley General y 12 de los Lineamientos Generales o los que correspondan en las legislaciones estatales en la materia. Lo anterior, siempre y cuando, de conformidad con la Ley General, los Lineamientos Generales y demás normatividad que resulta aplicable o con las legislaciones estatales en la materia y demás ordenamientos derivados, el consentimiento de los titulares, según sea el caso, sea exigible al no actualizarse alguna causal de excepción.
- Se recomienda que por lo que hace al tratamiento de datos personales de los sistemas 4, 5 y 6, establecer mecanismos, procesos y controles administrativos y técnicos para garantizar la calidad los datos personales que permitan que los datos personales sean exactos, completos y actualizados en función de la naturaleza de la información.
- Se recomienda establecer mecanismos, procesos y controles administrativos y técnicos para garantizar la calidad los datos personales que permitan que los datos personales sean actualizados en función de la naturaleza de la información respecto de los sistemas 1, 2 y 3.
- Asimismo, con independencia de que sean los encargados los responsables de alimentar las bases que conforman los sistemas de la PDN, y en este sentido sean quienes en primera instancia cumplan con el principio de calidad, la SESNA como administradora de la plataforma deberá asegurarse que la configuración de la interoperabilidad y los accesos a las bases de datos de los distintos sistemas por medio de las APIs, garantice que dicha consulta se efectúe respecto a las bases en su última versión, es decir aquella con la información más actualizada.
- Se sugiere contemplar métodos y/o técnicas para garantizar el borrado de los datos de navegación al no incluir evidencias que den soporte a las manifestaciones realizadas sobre un proceso de anonimización de los datos utilizados para fines estadísticos y los reportes e información de análisis que genere la PDN.
- La SESNA deberá a poner a disposición un aviso de privacidad del tratamiento de datos personales que realice con la implementación de la PDN, el cual se trata de un documento diferente a los Términos y Condiciones de Uso de la PDN, que fueron referidos en la evaluación de impactado presentada.
- En cumplimiento con el principio de información y la puesta a disposición del aviso de privacidad correspondiente, en el que se informe al titular la existencia y características

principales del tratamiento al que serán sometidos sus datos personales de conformidad con a lo dispuesto en la Ley General y Lineamientos Generales, deberá considerarse la interacción de los sistemas de la PDN con y los diversos subsistemas con los que interactúa.

- Implementar los mecanismos y controles concretos que consideren pertinentes y que tengan por objeto acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la Ley General, los Lineamientos Generales y demás normatividad aplicable.
- De manera particular, se recomienda poner especial atención a la implementación de los mecanismos para la protección de datos personales por diseño y por defecto, en la implementación de la PDN.
- En términos de lo que previene el artículo 30 de la Ley General, se sugiere identificar la evidencia del cumplimiento del principio de responsabilidad en torno a:
    - Se destinan recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales.
    - Se cuenta con políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable.
    - Se pone en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.
    - Se revisan periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.
    - Se establece un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
    - Se establecen procedimientos para recibir y responder dudas y quejas de los titulares; así mismo, definir en el marco de dichos procedimientos la vinculación con la gestión de cambios en la PDN, como parte del soporte técnico, mesa de ayuda, y, la gestión de la experiencia de las y los usuarios, así como entidades relacionadas.
    - Se diseñan, desarrollan e implementan sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la Ley General y las demás que resulten aplicables en la materia.
    - Se garantiza que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplen por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.

3. Deber de seguridad

- En términos de lo previsto por el artículo 34 de la Ley General, se sugiere a la SESNA generar evidencia de la implementación de un Sistema de Gestión, y, del cumplimiento de lo establecido en los diversos artículos 31, 32 y 33 de la Ley General, ya que si bien, se remite un documento de seguridad, se advierte que éste es específico para la PDN y no se identifica dicho tratamiento dentro del marco del Sistema de Gestión de la SESNA. Así mismo, a pesar de existir disposición expresa que obliga a la SESNA en las Bases para el funcionamiento de la PDN, no se acompañó evidencia, o se acompañó evidencia parcial, de los requerimientos normativos a que hacen referencia los numerales 6 (protocolos, estándares, reglamentos, especificaciones técnicas y cualquier normativa necesaria para la colaboración, provisión de datos y acciones para cumplir con las Bases), 12, 13, 14, 15, 16, 17, 18, 19, 22, 23, 24, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37 y 38.
- En términos de lo establecido por los artículos 30, fracción II, y 33, fracción I, de la Ley General, valorar el establecimiento de un Programa de Protección de Datos Personales al interior de la SESNA que comprenda todos los tratamientos de datos personales a su cargo, con independencia de las acciones específicas en torno a la PDN, con independencia de en el marco del mismo pueda definir, monitorear, evaluar y mejorar en torno a:
    - La elaboración de políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable.
    - La creación de políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.
- En términos de lo previsto por el artículo 35 de la Ley General, se sugiere:
    - Incorporar de conformidad con el artículo 35, fracción I, los sistemas y subsistemas de tratamiento de entrada o de salida de la información, interacciones que no se encuentran reportadas en el documento de seguridad.
    - En términos de la identificación de actores involucrados que se desprende de la identificación de los sistemas de tratamiento requerida en términos del artículo 35, fracción I, de la Ley General, en la determinación de los perfiles y catálogos de usuarios deberán señalarse las funciones y obligaciones y deberá confirmarse que las responsabilidades en torno al adecuado manejo de la PDN resultan exigibles en términos de las disposiciones legales aplicables. En el ámbito
    - En términos de la identificación de actores involucrados que se desprende de la identificación de los sistemas de tratamiento requerida en términos del artículo 35, fracción I, de la Ley General, con independencia de las funciones y obligaciones de carácter genérico que se reconocen en el tratamiento, se sugiere identificar las que corresponden de manera específica a las entidades, sistemas y subsistemas con los que interopera la PDN, a fin de confirmar o descartar obligaciones específicas en función de entidad involucrada o de perfil de usuario. Derivado de lo anterior, deberá

confirmarse que se cuentan con todos los requerimientos legales y en su caso, documentos particulares, que permitan exigir responsabilidad proactiva de todas las personas que realizan alguna operación dentro de la PDN, o inclusive, de aquellos con los que interopera.

- En términos de la elaboración del inventario de datos personales, los sistemas de tratamiento y la identificación de actores involucrados que se desprende de la identificación de los sistemas de tratamiento requerida en términos del artículo 35, fracción I, de la Ley General, definir en términos técnicos y normativos en qué consiste el tratamiento de datos personales, consistente en "inteligencia" a que hace referencia el artículo 4 de las Bases para el funcionamiento de la PDN, a fin que, de identificarse un tratamiento de datos personales potencial como parte del funcionamiento de la PDN, éste sea identificado y gestionado dentro del Plan de Trabajo a que hace referencia el artículo 35, fracción V, de la Ley General, previa elaboración de un análisis de brecha.
- En términos de la elaboración del inventario de datos personales, los sistemas de tratamiento y la identificación de actores involucrados que se desprende de la identificación de los sistemas de tratamiento requerida en términos del artículo 35, fracción I, de la Ley General, con relación al diverso 35, fracción VI, de la Ley General, relativo a incluir los mecanismos de monitoreo y revisión de las medidas de seguridad; la SESNA deberá identificar:
    - Las medidas de seguridad implementadas a través de los controles específicos por los cuáles éstas se gestionen.
    - La eficacia de su implementación, para lo cual, podrá vincularse de manera enunciativa con los resultados de los análisis de riesgo y de brecha.
    - Los documentos que soporten la medición, análisis y mejora de las medidas de seguridad implementadas.
    - Los informes y comunicaciones derivados de la implementación de las medidas de seguridad.
    - Los informes y comunicaciones derivados del desempeño de la operación de la PDN, como un reflejo global de la adecuada implementación de las medidas de seguridad.
- En términos de la elaboración del inventario de datos personales, los sistemas de tratamiento y la identificación de actores involucrados que se desprende de la identificación de los sistemas de tratamiento requerida en términos del artículo 35, fracción I, se sugiere incorporar mecanismos de capacitación y comunicación con todos los perfiles involucrados a través de la generación de capacitaciones, tutoriales, y cualquier tipo de herramienta de capacitación y adiestramiento para todos los actores que vayan a tener interacción con la PDN, a fin de que se advierta que el

Programa General de Capacitación, no solamente considera los niveles de capacitación, sino los contenidos en función de los roles y responsabilidades apropiadas para su manejo.

- Se recomienda dejar evidencia de que cada sistema es responsabilidad del propietario, así como resultados de pruebas que demuestren la seguridad de la comunicación entre sistemas y plataforma que indiquen que no hay riesgos hacia los sistemas por la comunicación desde la plataforma, garantizando la integridad de los datos que se consultan y las bases de datos del propietario, dejando claro que la plataforma no representa riesgos y que, las amenazas que pudieran presentarse son conocidas y se pueden contener en caso de alguna vulneración.
- Realice un debido análisis de riesgos que le permita a la SESNA identificar las medidas de seguridad necesarias a implementar ya que, de acuerdo con la descripción, existen amenazas intrínsecas que no son reportadas ni mucho menos analizadas, por lo que se espera que se incluyan reportes que pongan en evidencia la seguridad de las comunicaciones entre sistemas y finalmente, la descripción de las medidas de seguridad administrativas y físicas que se identifiquen y acrediten respecto de la propia plataforma.

4. Deber de confidencialidad

- Se sugiere implementar algún tipo de control o mecanismo que tenga como propósito que todas las personas que intervengan en el tratamiento de los datos personales tratados a través de la PDN guarden confidencialidad respecto de tales datos personales, como la elaboración de cláusulas contractuales, elaboración de cartas compromiso, en general la elaboración de cualquier documento o instrumento que permita acreditar que el responsable cuenta con mecanismos que garanticen la confidencialidad de los datos personales que recaba, lo anterior, en términos de la identificación de los requerimientos a que hace referencia el artículo 35, fracciones I y II, de la Ley General.
- Determinar en términos del artículo 35, fracciones I, II y VI, de la Ley General, una verz que se hayan determinado catálogos y perfiles de usuarios y niveles de acceso, los mecanismos apropiados para gestionar los permisos de acceso y la tecnología relativa a la identificación y autenticación, a fin de llevar a cabo una gestión adecuada de la identidad de los usuarios y del registro de las operaciones que éstos realizan en cada sesión, con independencia de los demás mecanismos inherentes a la información que se registrará en dichas sesiones, considerando de manera integral cualquier uso potencial de los datos personales sujetos de tratamiento.

5. Encargado

- En el marco de lo establecido por el artículo 35, fracciones I y II, de la Ley General en el marco de la elaboración del inventario de datos personales, los sistemas de tratamiento y la

identificación de actores involucrados que se desprende de la identificación de los sistemas de tratamiento; se sugiere identificar la distinción entre responsable y encargado en términos de lo que previene la Ley General, así como de las comunicaciones de datos, sean transferencias y/o remisiones, según correspondan, y, señalar similitudes y diferencias con los conceptos que se utilizan en el marco de la aplicación de las disposiciones de la Ley General del SNA y las Bases de funcionamiento de la PDN.

- En su caso, deberá contratar o adherirse a servicios de cómputo en la nube y otras materias que garanticen políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la Ley General, los Lineamientos Generales y demás normatividad derivada.

6. Transferencias

- Deberá identificar y documentos las reglas establecidas en los artículos 65, 66, 67, 68, 69 y 70 de la Ley General y 113, 114 115 y 116 de los Lineamientos Generales, así como las excepciones.

IX. Consideraciones finales.

PRIMERA. En términos de lo señalado en el apartado II, el presente dictamen se emite con la salvedad de que para su emisión se tomaron en cuenta los datos e información proporcionada por la SESNA, por lo que la responsabilidad respecto a las manifestaciones, abstenciones o eventuales omisiones, son responsabilidad exclusiva de la SESNA como sujeto obligado en términos del artículo 1 párrafo quinto de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y del artículo 30 párrafo segundo de las Disposiciones administrativas.

SEGUNDA. La Dirección General de Normatividad y Consulta, en términos de lo previsto por los artículos 32 de las Disposiciones administrativas, y 42 fracción V del Estatuto Orgánico, queda a su disposición para asesorarle en la implementación de los resultados del presente dictamen de la evaluación de impacto en la protección de datos personales, en el entendido que, de considerarlas pertinentes, lleve a cabo su implementación a la brevedad respecto de las que resulte factible su implementación, así como aquellas, que por el momento no puedan ser implementadas, pero sí registradas dentro del Plan de Trabajo o Programa de Protección de Datos Personales que corresponda.

TERCERA. Considerando que las actuaciones generadas en el presente expediente son susceptibles de constituir información clasificada, se solicita atentamente a la SESNA, para que indique lo siguiente:

- Describa o señale de manera especifica la información susceptible de constituir información clasificada, ya sea reservada o confidencial.
- Señale la causal o causales de clasificación que correspondan en términos de los artículos 110 y/o 113 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el supuesto especifico que corresponda conforme a los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, correlacionándolo con la información que corresponda en términos del punto que precede.
- Indique de manera general, las razones, motivos, circunstancias y/o fundamento que soportarían la clasificación de referencia.
- En caso de tratarse de información reservada, señalar el periodo relativo a la misma.

Lo anterior, con la prevención de que esta unidad administrativa podrá considerar la totalidad de la información contenida en el expediente como información pública, con excepción de los datos personales confidenciales y las medidas de seguridad que a consideración de esta unidad administrativa deban reservarse por encontrarse en la hipótesis prevista por el artículo 110, fracción VII, de la Ley Federal de Transparencia y Acceso a la Información Pública, como información relativa a la prevención de potenciales delitos.

CUARTA. Se ponen a disposición las documentales proporcionadas para la tramitación del Dictamen relativo a la Evaluación de Impacto en la Protección de Datos Personales de la puesta en operación de la PDN, a efecto de que el sujeto obligado pueda solicitar la devolución de las mismas, las cuales podrán ser recogidos en las oficinas de este Instituto, a través de la persona que se autorice para tal efecto, o bien, de así requerirlo, le sean enviados por mensajería al domicilio del sujeto obligado, para lo cual se solicita que se indiquen el nombre y cargo de la persona que recibirá dicha documentación, así como cualquier otra medida de seguridad que resultara exigible sobre el particular. En caso de que dicha información no sea devuelta al presentante, esta unidad administrativa procederá a su destrucción mediante mecanismos seguros de borrado de conformidad con sus instrumentos de control archivístico que resultan aplicables a la serie documental *"Evaluaciones de impacto en la protección de datos personales en posesión de sujetos obligados"*.

El presente documento se emite en términos de lo dispuesto por los artículos 25, primer párrafo, fracción XIII, segundo párrafo, 29 fracciones XXX y XL, y, 42 fracciones IV y XII del Estatuto Orgánico, por parte del Director General de Normatividad y Consulta, Luis Ricardo Sánchez Hernández.

VMCB/PRR-MTLM/PHM