# DOCUMENTO DE SEGURIDAD DE LA SECRETARÍA EJECUTIVA DEL SISTEMA NACIONAL ANTICORRUPCIÓN

# UNIDAD DE SERVICIOS TECNOLÓGICOS Y PLATAFORMA DIGITAL NACIONAL

2022

## CONTENIDO.

## 1. INTRODUCCIÓN

El 27 de mayo de 2015 se publicó en el Diario Oficial de la Federación (**DOF**) el "Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos (**CPEUM**), en materia de combate a la corrupción", mediante el cual se reformó, entre otros, el artículo 113 constitucional, instituyéndose el Sistema Nacional Anticorrupción (**SNA**) como 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.

En ese orden de ideas, por Decreto del Titular del Poder Ejecutivo Federal, publicado en el **DOF** el 18 de julio de 2016, se expidió la Ley General del Sistema Nacional Anticorrupción (**LGSNA**), cuyo artículo 24 dispone la creación de un organismo descentralizado, no sectorizado, con personalidad jurídica y patrimonio propio, con autonomía técnica y de gestión, con sede en la Ciudad de México, denominado Secretaría Ejecutiva del Sistema Nacional Anticorrupción (**SESNA**).

La **SESNA** es un órgano de apoyo técnico del Comité Coordinador del Sistema Nacional Anticorrupción, a efecto de proveerle la asistencia técnica, así como los insumos necesarios para el desempeño de sus atribuciones, conforme a lo dispuesto en la fracción III del artículo 113 de la **CPEUM** y la **LGSNA**. Además, administrará la Plataforma Digital Nacional[1] (**PDN**).

Por otra parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (**LGPDPPSO**), publicada en el **DOF** el 26 de enero de 2017, es un instrumento de orden público y de observancia general en toda la República, reglamentaria de los artículos 6º, Base A y 16, párrafo segundo, de la **CPEUM**.

El objeto de la **LGPDPPSO** consiste en establecer bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados; entre los cuales se encuentra la **SESNA**.

Por lo tanto, esta Secretaría está constreñida al cumplimiento de diversas obligaciones legales relacionadas con el tratamiento de los datos personales que se deriven del ejercicio de sus facultades, las cuales deben apegarse a los principios y deberes que establece dicha Ley.

La **SESNA** debe observar los principios de *licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad* en el tratamiento de datos personales, además de asegurar que dicho tratamiento esté justificado por finalidades concretas lícitas, explícitas y legítimas, establecidas en sus avisos de privacidad respectivos, el cual debe consentir el titular de los datos de manera libre, específica e informada, ya sea de forma expresa o tácita.

[1] Artículo 48 de la LGSNA.

Asimismo, la **SESNA** debe adoptar las medidas necesarias para que los datos personales en su posesión se mantengan exactos, completos, correctos y actualizados a fin de que no se altere la veracidad de éstos, así como establecer mecanismos para cumplir con el principio de responsabilidad establecido en la **LGPDPPSO**.

Además, la **SESNA** debe establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales que posee, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deben estar documentadas y contenidas en un sistema de gestión y de manera particular, la **SESNA** tiene la obligación de elaborar un documento de seguridad, el cual es un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

En cumplimiento a la **LGPDPPSO**, a continuación, se presenta el Documento de Seguridad elaborado por la **SESNA**, mismo que resulta de observancia obligatoria para la operación y administración de la Plataforma Digital Nacional.

## 2. GLOSARIO

Para efectos del presente Documento de Seguridad, se entenderá por:

- **Áreas:** Instancias que integran la unidad administrativa que de acuerdo con la normatividad puedan tener en sus archivos la información y los datos personales.

- **Aviso de privacidad:** Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por la autoridad que recabe los datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

- **Bases de datos:** Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

- **Base de la PDN:** Bases para el funcionamiento de la Plataforma Digital Nacional, publicadas en el DOF el 23 de octubre de 2018. Estas Bases 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;

- **Bloqueo:** La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

- **Comité de Transparencia:** Instancia a la que hacen referencia los artículos 43 de la Ley General de Transparencia y Acceso a la Información Pública y 64 de la Ley Federal de Transparencia y Acceso a la Información Pública.

- **Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

- **Consentimiento:** Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de estos.

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

- **Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

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

- **Disociación:** El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

- **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por la Secretaría Ejecutiva del Sistema Nacional Anticorrupción para la administración y operación de la Plataforma Digital Nacional.

- **Encargado:** toda persona o ente que recibe ordena o resguarda datos e información en los subsistemas para su integración a los sistemas que forman la Plataforma Digital Nacional, de acuerdo con el artículo 3, fracción X de las Bases para el funcionamiento de la PDN.

- **Instituto o INAI:** Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados.

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

- **LGSNA:** Ley General del Sistema Nacional Anticorrupción

- **-LGRA:** Ley General de Responsabilidades Administrativas

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

- **Medidas de seguridad administrativas:** Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

- **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

  a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
  b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
  c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
  d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

- **Medidas de seguridad técnicas:** Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
  a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
  b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
  c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
  d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

- **Organismos garantes:** Aquellos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales, en términos de los artículos 6° y 116, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos.

- **PLataforma Digital Nacional (PDN):** 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.

- **Plataforma Nacional:** La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública.

- **Remisión:** Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

- **Responsable:** Los sujetos obligados a que se refiere el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que deciden sobre el tratamiento de datos personales.

- **SESNA**: Secretaría Ejecutiva del Sistema Nacional Anticorrupción, organismo descentralizado no sectorizado, con personalidad jurídica y patrimonio propio, con autonomía técnica y de gestión; que tiene por objeto fungir como órgano de apoyo técnico del Comité Coordinador del Sistema Nacional Anticorrupción, a efecto de proveerle asistencia técnica, así como los insumos necesarios para el desempeño de sus atribuciones constitucionales y legales.

- **Sistema de Tratamiento de Datos Personales:** Constituye el conjunto ordenado de datos personales que están en posesión de alguna de las áreas de la **SESNA** con independencia de su forma de acceso, creación, almacenamiento u organización.

Existen dos tipos de sistemas de tratamiento de datos personales:

1) **Físicos**, que son un conjunto ordenado de datos que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos; y
2) **Automatizados**, conjunto ordenado de datos que para su tratamiento han sido o están sujetos a un tratamiento informático y que por ende requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.

- **Supresión:** La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable.

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

- **Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

- **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.

- **Unidades administrativas:** Las señaladas en el artículo 9 del Estatuto Orgánico de la Secretaría Ejecutiva del Sistema Nacional Anticorrupción;

- **Unidad de Transparencia:** Instancia a la que hacen referencia los artículos 45 de la Ley General de Transparencia y Acceso a la Información Pública y 61 de la Ley Federal de Transparencia y Acceso a la Información Pública.

- **USTPDN:** Unidad de Servicios Tecnológicos y Plataforma Digital Nacional.

## 3. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO DE LA PLATAFORMA DIGITAL NACIONAL

### a. 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:

| SISTEMA DE TRATAMIENTO DATOS PERSONALES DEL S1 | | |
|---|---|---|
| Inventario de Datos Personales | | |
| *Nivel Estándar* | | |
| *Tipo de Datos Personales* | *Documentos* | *Datos Personales* |
| Datos de identificación del declarante. | - Formatos de declaraciones: de situación patrimonial y de intereses. | - Nombre<br>- RFC<br>- CURP<br>- Estado civil<br>- Lugar de nacimiento<br>- Fecha de nacimiento<br>- Nacionalidad<br>- Firma<br>- Dependientes<br>- Beneficiarios |
| Datos laborales del declarante. | - Formatos de declaraciones: de situación patrimonial y de intereses. | - Escolaridad<br>- Puesto de trabajo<br>- Experiencia laboral<br>- Años laborados |
| Datos patrimoniales del declarante. | - Formatos de declaraciones: de situación patrimonial y de intereses. | - Ingresos netos del declarante<br>- Bienes Inmuebles<br>- Bienes muebles<br>- Inversiones, Cuentas Bancarias y otro tipo de Valores/Activos<br>- Adeudos/Pasivos del declarante<br>- Participación en empresas, sociedades, asociaciones<br>- Apoyos o beneficios públicos<br>- Beneficios privados, y |

| | | |
|---|---|---|
| | | - Fideicomisos. |
| Datos de contacto del declarante. | - Formatos de declaraciones: de situación patrimonial y de intereses. | - Correo electrónico particular<br>- Número de teléfono particular<br>- Número de teléfono celular particular<br>- Domicilio particular |
| ***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<br>- RFC<br>- Estado civil o parentesco con el declarante.<br>- Lugar de nacimiento<br>- Fecha de nacimiento<br>- Nacionalidad<br>- Domicilio |
| Datos de patrimoniales de la pareja o dependientes económicos del declarante. | - Formatos de declaraciones: de situación patrimonial y de intereses. | - Ingresos netos<br>- Bienes Inmuebles<br>- Bienes muebles<br>- Inversiones, Cuentas Bancarias y otro tipo de Valores/Activos<br>- Adeudos/Pasivos<br>- Participación en empresas, sociedades, asociaciones<br>- Apoyos o beneficios públicos<br>- Beneficios privados<br>- Fideicomisos. |

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. Su funcionamiento se basa en servicios web o API's para consultar la información de los servidores y las bases de datos de los Encargados, y los refleja en la Plataforma.

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. Las finalidades de este sistema de información son:

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, sustanciadores 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 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.

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.

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.

b. **Sistema de Tratamiento de Datos Personales del Sistema de los Servidores públicos que intervengan en procedimientos de contrataciones públicas (en lo sucesivo, S2)**

Datos personales contenidos en el sistema:

| SISTEMA DE TRATAMIENTO DE DATOS PERSONALES DEL S2 | | |
|---|---|---|
| Inventario de Datos Personales | | |
| *Nivel Estándar* | | |
| *Tipo de Datos Personales* | *Documentos* | *Datos Personales* |
| Datos de identificación de la persona servidora pública: | - Información contenida en los sistemas de contrataciones públicas | - Nombre<br>- Nombre de la persona servidora pública que funge como superior jerárquico.<br>- RFC<br>- CURP<br>- RFC de la persona servidora pública que funge como superior jerárquico.<br>- CURP persona servidora pública que funge como superior jerárquico. |

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.

c. **Sistema de Tratamiento de Datos Personales del Sistema nacional de Servidores públicos y particulares sancionados (en lo sucesivo, S3)**

Datos personales contenidos en el sistema:

| SISTEMA DE TRATAMIENTO DE DATOS PERSONALES DEL S3 | | |
|---|---|---|
| **Inventario de Datos Personales** | | |
| ***Nivel Estándar*** | | |
| *Tipo de Datos Personales* | *Documentos* | *Datos Personales* |
| Datos de identificación de la persona servidora pública: | - Sistemas de Registro de Servidores Públicos Sancionados | - Nombre<br>- Género<br>- RFC<br>- CURP |

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.

d. **Sistema de Tratamiento de Datos Personales del Sistema de información pública de contrataciones (S6)**

Datos personales contenidos en el sistema:

| SISTEMA DE TRATAMIENTO DE DATOS PERSONALES DEL S6 | | |
|---|---|---|
| **Inventario de Datos Personales** | | |
| ***Nivel Estándar*** | | |
| *Tipo de Datos Personales* | *Documentos* | *Datos Personales* |
| Datos de identificación: | - Información contenida en los sistemas de contrataciones públicas | - Nombre de las personas servidoras públicas que intervienen en los procedimientos de contrataciones públicas.<br>- Nombre de las personas físicas que participan en procedimientos de contrataciones públicas.<br>- Nombre de las personas físicas a las que se les adjudica un contrato público. |

*Para los sistemas de tratamiento de datos personales S2, S3 y S6 aplica lo siguiente:*

Al ser sistemas de consulta pública, cualquier persona podrá acceder a esta información. Se aclara que esta información actualmente se encuentra en bases de datos públicas y la PDN únicamente será una herramienta que permite la interoperabilidad de sistemas, estandarización de datos y homologación de procesos.

*Para el sistema de tratamientos de datos personales S1*

De acuerdo con el "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 el 16 de noviembre de 2018 en el Diario

Oficial de la Federación y, posteriormente, 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[2] habrá información contenida en este sistema que será pública y otra que será reservada.

Por lo tanto, se 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 y se establecerá un mecanismo exclusivo para que las autoridades competentes accedan a la información reservada.

*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.

[2] https://www.dof.gob.mx/nota_detalle.php?codigo=5573194&fecha=23/09/2019

## 4. FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.

Para todos los sistemas de tratamiento de datos personales aplica lo siguiente:

<table>
<tr><th colspan="2">SISTEMA DE TRATAMIENTO DATOS PERSONALES<br>DEL S1, S2, S3 y S6</th></tr>
<tr><th>Área que opera el sistema:</th><th>Sistema</th></tr>
<tr><td>Dirección de Desarrollo y Evaluación de la Plataforma Digital Nacional</td><td>S1</td></tr>
<tr><td>Dirección de Sistemas de Información</td><td>S2</td></tr>
<tr><td>Dirección de Interoperabilidad de Sistemas de Información</td><td>S3</td></tr>
<tr><td>Dirección de Sistemas de Información</td><td>S6</td></tr>
<tr><td colspan="2">Funciones:<br><br>La USTPDN es responsable de asegurar el adecuado funcionamiento de los Sistemas de la PDN, así como de supervisar que existe una conexión funcional con los Encargados de la información.<br>La USTPDN registra e informa sobre cualquier incidente en términos de una falla en la comunicación con la PDN.<br>La USTPDN realiza la evaluación, implementación, mantenimiento y actualización de los componentes informáticos de la Plataforma.<br><br>La USTPDN desarrolla proyectos estratégicos en materia de informática y tecnologías de la información, análisis de datos e inteligencia para el cumplimiento de los objetivos del Sistema Nacional Anticorrupción.<br><br>La USTPDN presenta informes al Comité Coordinador sobre las mejoras realizadas a la Plataforma.</td></tr>
<tr><td>Servidor público responsable del debido tratamiento de los datos personales:</td><td>● Dirección de Desarrollo y Evaluación de la Plataforma Digital Nacional<br>● Dirección de Sistemas de Información<br>● Dirección de Interoperabilidad de Sistemas de Información<br>● Dirección de Sistemas de Información</td></tr>
<tr><td colspan="2">Funciones y Obligaciones:<br>Implementar acciones que permitan el mejor funcionamiento y una mejor contínua en la operación y los sistemas de la PDN.<br>Garantizar que la PDN cuente con los controles y protocolos adecuados para el manejo y comunicación con los Encargados.<br>Revisar continuamente el buen uso y funcionamiento de la PDN.<br>Atender y dar seguimiento a las consultas de usuarios y Encargados en términos de transferencia de información o uso de los datos.<br>Organizar los servicios de la PDN para garantizar que se cumpla con la normatividad y legislación aplicable.</td></tr>
</table>

## 5. ANÁLISIS DE RIESGOS.

[redacted]

Se testa del documento la sección "Mecanismos de Seguridad" "Análisis de riesgos", "Análisis de brecha" y " Plan de trabajo" por considerarse información de carácter reservada de conformidad con el artículo 110 fracción VII de la **LFTAIP** y Vigésimo Sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

[redacted]

[redacted]

[redacted]

| [redacted] | [redacted] |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

[redacted]

[redacted]

[redacted]

| [redacted] | [redacted] |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

- [redacted]

[redacted]

[redacted]

| [redacted] | [redacted] |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

[redacted]

[redacted]

| [redacted] | [redacted] |
|---|---|
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| [redacted] | [redacted] |

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]

- [redacted]

- [redacted]
  - [redacted]
  - [redacted]

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

- [redacted]

- [redacted]
- [redacted]

  [redacted]

- [redacted]
- [redacted]

## 6. ANÁLISIS DE BRECHA.

[redacted]

## 7. PLAN DE TRABAJO

[redacted]

[redacted]

| [redacted] | | |
|---|---|---|
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |
| [redacted] | [redacted] | [redacted] |

## 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 auditoría, 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.