DOCUMENTO DE SEGURIDAD PARA LA PLATAFORMA DEL SISTEMA ESTADÍSTICO NACIONAL DE PROCURACIÓN DE JUSTICIA

INTRODUCCIÓN

La integridad y confidencialidad de la información almacenada en el Sistema Estadístico Nacional de Procuración de Justicia son fundamentales. En este sentido, se han establecido las medidas y mecanismos de seguridad necesarios que garantizan el resguardo, la protección y el tratamiento de la información. Bajo este contexto y con el objetivo de salvaguardar la privacidad de los individuos, en enero de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en adelante Ley General, la cual tiene como propósito establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales que estén en posesión de los sujetos obligados.

Al respecto, en su artículo primero, la Ley General señala que son sujetos obligados, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, **órganos autónomos**, partidos políticos, fideicomisos y fondos públicos.

La Fiscalía General de la República (**FGR**), como órgano autónomo encargado de investigar y perseguir delitos de orden federal[1] con carácter de sujeto obligado, tiene el deber de proteger los datos personales en su posesión, e implementar mecanismos que acrediten el cumplimiento a los principios, deberes, derechos y demás obligaciones establecidas en Ley General, de acuerdo con sus atribuciones.

Por otra parte, de conformidad con lo dispuesto en los artículos 29 y 30, fracciones I y VII de la Ley General, se deberán implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en dicha Ley, aunado a lo anterior, dispone que el tratamiento de datos personales que realicen los sujetos obligados estará regido por ocho principios y dos deberes, teniendo como principios el de licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad y responsabilidad; mientras que los dos deberes son el de confidencialidad y seguridad. Estos principios, deberes y derechos imponen una serie de obligaciones para los sujetos regulados por la Ley General, cuya finalidad es que el tratamiento se realice garantizando la protección de los datos personales, con el objeto de respetar el derecho a la autodeterminación informativa de los titulares.

Que el 6 de diciembre de 2019 en la XLII Asamblea Plenaria de la Conferencia Nacional de Procuración de Justicia (CNPJ), mediante acuerdo CNPJ/XLII/04/2019 se acordó la creación del Sistema Estadístico Nacional de Procuración de Justicia (SENAP), a efecto de contar con información estadística de calidad mediante la homologación del registro, procesamiento y difusión de la información contenida en las carpetas de investigación

[1] *Artículo 21 y 102 de la CPEUM*

respecto de los hechos presuntamente delictivos, víctimas, personas imputadas y estado procesal de las mismas.

Que en el marco de los trabajos de la CNPJ se estableció que el INEGI será el encargado de la gobernanza del SENAP, incluida la coordinación conceptual y metodológica del mismo con fines estadísticos, que, la adopción correspondería a las instituciones de procuración de justicia, en coordinación con la FGR, siendo esta última la encargada del resguardo, almacenamiento y seguridad tecnológica, en términos de la normatividad aplicable.

Que la Conferencia Nacional de Procuración de Justicia, en el marco de la XLV Asamblea Plenaria, aprobó el proyecto de Norma Técnica del Sistema Estadístico Nacional de Procuración de Justicia, mediante acuerdo CNPJ/XLV/01/2021.

Que la Junta de Gobierno del Instituto Nacional de Estadística y Geografía aprobó la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia, en términos del Acuerdo 16ª/IV/2023, aprobado en su Décima Sexta sesión, celebrada el 31 de octubre de 2023.

Que el Acuerdo por el que se aprueba la Norma Técnica para la Producción de Información del Sistema Nacional de Procuración de Justicia se publicó en el Diario Oficial de la Federación el 10 de noviembre de 2023 y es de observancia obligatoria para las Unidades del Estado que intervengan o participen en el proceso de producción de información del SENAP.

Que el artículo 23 de la Norma técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia, señala que "La seguridad de la información de la base de datos estará a cargo de la Fiscalía General de la República, a través de la Agencia de Investigación Criminal, la cual tendrá a su cargo el almacenamiento de los datos y deberá garantizar la implementación de las medidas y mecanismos de seguridad necesarios para el resguardo, protección, confidencialidad y cuidado de la información, para lo cual emitirá el documento de seguridad correspondiente, apegándose a la Política para la Gestión de la Confidencialidad en la Información Estadística y Geográfica".

Que los artículos 37, 38, 40, 41, 46 y 47 de la Ley del Sistema Nacional de Información Estadística y Geográfica, de observancia general en toda la República, establecen obligaciones de las Unidades del Estado para garantizar la estricta confidencialidad de los datos que se les proporcionen con fines estadísticos y evitar su uso para cualquier otro fin.

Que los artículos 103, 104 y 105 de la LGSNIEG establecen las infracciones imputables a las personas servidoras públicas del INEGI o de las Unidades del Estado, mientras que los artículos 106, 107, 108, 109, 110, 111 y 112 de la LSNIEG determinan las sanciones correspondientes.

Que la Política para la Gestión de la Confidencialidad en la Información Estadística y Geográfica, publicada el 29 de octubre de 2021 en el Diario Oficial de la Federación, de observancia general y obligatoria para las Unidades del Estado, establece las medidas generales que se deben implementar para gestionar la confidencialidad estadística de los datos que recaban con fines estadísticos y evitar su uso para cualquier otro fin.

En esas consideraciones, el artículo 35 de la Ley General establece como una obligación la elaboración de un **documento de seguridad**, que de conformidad con la fracción XIV del artículo 3 de la Ley antes referida se define como el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

El cual, deberá contener al menos la siguiente información:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

DEBER DE SEGURIDAD

De conformidad con lo establecido en el artículo 31 de la Ley General, con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable tendrá el deber de 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.

- Garantizar su confidencialidad, integridad y disponibilidad.

En esas consideraciones, el artículo 35 de la Ley General, dispone de manera particular en atención a dichas medidas la elaboración de un Documento de Seguridad.

Por lo que, en atención al deber de seguridad de los datos personales, en los sistemas de tratamiento de datos personales de la Fiscalía General de la República se debe atender lo siguiente:

OBJETIVO

Garantizar la implementación de las medidas y mecanismos de seguridad necesarios para el resguardo, protección, confidencialidad y cuidado de la información, con apego a la Política para la Gestión de la Confidencialidad en la Información Estadística y Geográfica.

ÁMBITO DE APLICACIÓN

Respecto a los deberes que hace referencia la Ley General, este documento es aplicable para todas las unidades administrativas pertenecientes la FGR que, en el ejercicio de sus funciones y atribuciones, lleven a cabo una administración de bases de datos en el SENAP.

De igual forma, serán aplicables al tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento u almacenamiento.

Todos los servidores públicos que dentro de sus atribuciones tengan acceso a los datos personales así como al tratamiento de los mismos en cualquiera de sus fases, estarán obligados a conocer y aplicar las medidas de seguridad propias de cada sistema en el que se concentren los datos, observando en todo momento los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el

tratamiento de datos personales, tal como lo establece el artículo 16[2] de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

METODOLOGÍA

La integración de las obligaciones y responsabilidades establecidas en el Documento de Seguridad para la Plataforma del Sistema Estadístico Nacional de Procuración de Justicia incorpora los deberes de las áreas responsables, así como los de la Unidad Especializada en Transparencia y Apertura Gubernamental. Estas áreas llevarán a cabo las acciones correspondientes dentro de su ámbito de competencia, garantizando la adecuada protección de los datos personales.

Por parte de la Unidad Especializada de Transparencia y Apertura Gubernamental:

I. Establecer comunicación con las áreas responsables, con el propósito de llevar a cabo las actividades necesarias para la elaboración de su documento de seguridad correspondiente.
II. Brindar acompañamiento a las áreas para el cumplimiento de los Deberes.
III. Elaborar materiales de apoyo (manuales, guías, formatos, metodologías, procedimientos) para la generación del Documento de Seguridad.
IV. Llevar a cabo cursos y capacitaciones en materia de protección de datos personales con enfoque en seguridad, durante toda la ejecución de las actividades.
V. Dentro de cada reunión con las áreas correspondientes remite los puntos tratados, los compromisos adquiridos y los plazos para su cumplimiento.
VI. Llevar a cabo la revisión del Documento de Seguridad con la finalidad de que cumpla con todos los parámetros establecidos en el artículo 35 de la Ley General y, en su caso, emitir las observaciones pertinentes.

Por parte de las unidades administrativas responsables deberán:

I. Establecer comunicación con la Unidad Especializada de Transparencia y Apertura Gubernamental para dar seguimiento a las actividades de cumplimiento.
II. Hacer de conocimiento a la Unidad Especializada de Transparencia y Apertura Gubernamental el proceso de tratamiento de los datos personales.
III. Cumplir con los elementos que integran el documento de seguridad establecidos en el artículo 35 de la Ley General.
IV. Capacitar a su personal en materia de datos personales, con enfoque en seguridad de la información.
V. Remitir el documento del sistema de gestión de datos personales generado, a la Unidad Especializada de Transparencia y Apertura Gubernamental para su revisión y observaciones pertinentes.
VI. Presentar el documento ante el Comité de Transparencia, para fines de supervisión, mismo que será actualizado por el responsable cuando ocurran las hipótesis previstas dentro del artículo 36 de la Ley General.

[2] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en enero de 2017; Artículo 16. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

MEDIDAS DE SEGURIDAD DE LOS DATOS PERSONALES EN LA FISCALÍA GENERAL DE LA REPÚBLICA

Las medidas de seguridad de los datos personales se definen como el conjunto de acciones, actividades, controles o mecanismos que permiten proteger los datos frente a un daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, y garantizar con ello su confidencialidad, integridad y disponibilidad.

Esas medidas pueden ser de tipo administrativo, físicas y técnicas, las cuales, de conformidad con lo establecido en el artículo 3, fracciones XXI, XXII y XXIII de la Ley General, se describen a continuación:

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) Garantizar que el acceso a las bases de datos o a la información, así como a los recursos, sea sólo 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;

PRACTICAS EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

Como practicas generales, las personas servidoras públicas que lleven a cabo el tratamiento de datos personales, tienen que llevar a cabo lo siguiente:

- Tener su espacio de trabajo sin documentación importante a la vista.
- Cerrar los archiveros y resguardar la información personal bajo su custodia.
- Evitar dejar los documentos sobre impresoras.
- Realizar la eliminación segura de información en equipos de cómputo o cualquier otro medio de almacenamiento electrónico.
- Fijar plazos para la detención y eliminación de los datos personales en su posesión.
- Fomentar una cultura de la seguridad de la información.
- Bloquear o suspender las sesiones iniciadas en los equipos de cómputo.
- Cerciorarse del destinatario antes de enviar información.

SISTEMA DE DATOS PERSONALES: SISTEMA ESTADÍSTICO NACIONAL DE PROCURACIÓN DE JUSTICIA.

Unidad Administrativa	Nombre del Sistema de Datos Personales	Responsable del sistema de datos personales y cargo
Unidad Especializada de Infraestructura Tecnológica, Comunicaciones y Sistemas (UEITICS). **Subunidad de Tecnologías Aplicadas a la Investigación (SUTAI).** **Centro Federal de Inteligencia Criminal (CFIC).** **Secretaría Técnica de la Conferencia Nacional de Procuración de Justicia (STCNPJ).**	**SISTEMA ESTADÍSTICO NACIONAL DE PROCURACIÓN DE JUSTICIA (SENAP).**	Unidad Especializada de Infraestructura Tecnológica, Comunicaciones y Sistemas (UEITICS). *(nombre por definir)* Subunidad de Tecnologías Aplicadas a la Investigación (SUTAI). *(nombre por definir)* Centro Federal de Inteligencia Criminal (CFIC). *(nombre por definir)* Secretaría Técnica de la Conferencia Nacional de Procuración de Justicia (STCNPJ).

I. Inventario de datos personales

<table>
<tr><td>1. Finalidades del tratamiento</td><td>El tratamiento de los datos y la información contenida en este documento, deriva de lo establecido en el Capítulo IV, articulo 1, 5, 22 23, 24, 25, 26, 27 y 28 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia, publicada en el Diario Oficial de la Federación el 10 de noviembre de 2023; Título XI, Capitulo, articulo 261 al 265 del Estatuto Orgánico de la Fiscalía General de la República; Título Segundo, Capítulo V, Sección I, artículos 37, 38, , 46 y 47 de la Ley del Sistema Nacional de Información Estadística y Geográfica; así como artículos 1, 2, 4, 7 y 8 de la Política para la Gestión de la Confidencialidad en la Información Estadística y Geográfica.

Por lo anterior y derivado de la implementación del Sistema Estadístico Nacional de Procuración de Justicia, este tendrá por única finalidad generar información estadística, con el propósito de mejorar la calidad, disponibilidad y acceso a la información de la materia, a través de la homologación del registro, suministro, integración, resguardo, procesamiento, producción, publicación y difusión de la información de las denuncias y carpetas de investigación respecto de los hechos presuntamente delictivos, víctimas, personas imputadas y estado procesal de las mismas a cargo de las instituciones de procuración de justicia.</td></tr>
<tr><td>2. Catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales</td><td>Electrónicos: Los medios electrónicos de los cuales se obtienen los datos personales son las plantillas de carga de datos que corresponden a archivos CSV (comma separated values) en formato abierto el cual permite almacenar datos en forma de tablas las cuales son ingresadas al repositorio central del SENAP.

Físicos: Solicitud de acceso por parte de las instituciones que intervienen en la operación del SENAP ante la STCNPJ.</td></tr>
<tr><td>3. Catálogo de tipo de datos personales que se traten, indicando si son sensibles o no.

En relación con el artículo 32, fracción I y II de la LGPDPPSO.

(ISO 27001)</td><td>
<table>
<tr><th>Dato personal</th><th>Idoneidad de su captación (Diccionario de variables)</th><th>Finalidad</th></tr>
<tr><td colspan="3">Servidor Público solicitante</td></tr>
<tr><td colspan="3">Estándar</td></tr>
<tr><td>Cargo</td><td rowspan="6">Regular el proceso de producción de información estadística del Sistema Estadístico Nacional de Procuración de Justicia, con el propósito de mejorar la calidad, disponibilidad y acceso a la información de la materia, a través de la homologación del registro, suministro, integración, resguardo, procesamiento, producción, publicación y difusión de la información de las denuncias y carpetas de</td><td rowspan="6">1, 5, 18, 19, 20 y 25 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia</td></tr>
<tr><td>Dependencia</td></tr>
<tr><td>Corporación y/o Unidad de Adscripción</td></tr>
<tr><td>Teléfono institucional y /o extensión</td></tr>
<tr><td>Domicilio Institucional</td></tr>
<tr><td></td></tr>
</table>
</td></tr>
</table>

	Firma autógrafa	investigación respecto de los hechos presuntamente delictivos, víctimas, personas imputadas y estado procesal de las mismas a cargo de las instituciones de procuración de justicia.	
	Puesto		
	Nombre completo		
	Sensible		
	Domicilio	Regular el proceso de producción de información estadística del Sistema Estadístico Nacional de Procuración de Justicia, con el propósito de mejorar la calidad, disponibilidad y acceso a la información de la materia, a través de la homologación del registro, suministro, integración, resguardo, procesamiento, producción, publicación y difusión de la información de las denuncias y carpetas de investigación respecto de los hechos presuntamente delictivos, víctimas, personas imputadas y estado procesal de las mismas a cargo de las instituciones de procuración de justicia.	1, 5, 7, 18, 19, 20 y 25 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia

Dato personal	Idoneidad de su captación (Diccionario de variables)	Finalidad
Víctima		
Estándar		
Sexo	Regular el proceso de producción de información estadística del Sistema Estadístico Nacional de Procuración de Justicia, con el propósito de mejorar la calidad, disponibilidad y acceso a la información de la materia, a través de la homologación del registro, suministro, integración, resguardo, procesamiento, producción, publicación y difusión de la información de las denuncias y carpetas de investigación respecto de los hechos presuntamente delictivos, víctimas, personas imputadas y estado procesal de las mismas a cargo de las instituciones de procuración de justicia.	1, 5, 7, 11 y 14 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia
Edad		
Nacionalidad		
Nombre		
CURP		
Fecha de nacimiento		
Sensible		
Situación conyugal	Regular el proceso de producción de información estadística del Sistema Estadístico Nacional de Procuración de Justicia, con el propósito de mejorar la calidad, disponibilidad y acceso a la	1, 5, 7, 11 y 14 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia
Residencia habitual		

	Lengua extranjera	información de la materia, a través de la homologación del registro, suministro, integración, resguardo, procesamiento, producción, publicación y difusión de la información de las denuncias y carpetas de investigación respecto de los hechos presuntamente delictivos, víctimas, personas imputadas y estado procesal de las mismas a cargo de las instituciones de procuración de justicia.	
	Lengua indígena		
	Discapacidad		
	Alfabetismo		
	Escolaridad		
	Ocupación		
	Rango de ingresos		

Dato personal	**Idoneidad de su captación (Diccionario de variables)**	**Finalidad**
Persona imputada		
Estándar		
Edad	Regular el proceso de producción de información estadística del Sistema Estadístico Nacional de Procuración de Justicia, con el propósito de mejorar la calidad, disponibilidad y acceso a la información de la materia, a través de la homologación del registro, suministro, integración, resguardo, procesamiento, producción, publicación y difusión de la	1, 5, 7, 12 y 14 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia
Sexo		
Nacionalidad		
Nombre		
Alias		

	CURP	información de las denuncias y carpetas de investigación respecto de los hechos presuntamente delictivos, víctimas, personas imputadas y estado procesal de las mismas a cargo de las instituciones de procuración de justicia.	
	Fecha de nacimiento		
	Sensible		
	Situación conyugal	Regular el proceso de producción de información estadística del Sistema Estadístico Nacional de Procuración de Justicia, con el propósito de mejorar la calidad, disponibilidad y acceso a la información de la materia, a través de la homologación del registro, suministro, integración, resguardo, procesamiento, producción, publicación y difusión de la información de las denuncias y carpetas de investigación respecto de los hechos presuntamente delictivos, víctimas, personas imputadas y estado procesal de las mismas a cargo de las instituciones de procuración de justicia.	1, 5, 7, 12 y 14 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia
	Datos de nacimiento		
	Residencia habitual		
	Lengua extranjera		
	Lengua indígena,		
	Discapacidad		
	Alfabetismo, escolaridad		
	Ocupación		
	Rango de ingresos		

4. Catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales	**Medios de almacenamiento electrónico:** La infraestructura de procesamiento para el despliegue del SENAP en su versión transaccional y carga masiva de información, consistirá en servicios de aplicaciones, base de datos, así como de componentes especializados para el tratamiento de datos y su almacenamiento, estos componentes tecnológicos serán aprovisionados a través de la plataforma denominada Microsoft Azure, servicio que será suministrado por parte de la FGR a través de la Unidad Especializada de Infraestructura Tecnológica, Comunicaciones y Sistemas (UETICS) y administrado por la Subunidad de Tecnologías Aplicadas a la Investigación (SUTAI). El SENAP se encontrará ubicado en la infraestructura de almacenamiento de nube de la FGR. La STCNPJ remite las solicitudes de usuario y los compromisos de confidencialidad que reciba de parte de las instituciones de procuración de justicia y del INEGI al CFIC acompañadas del oficio correspondiente y almacenará una copia digital de las mismas, en la nube de la FGR. **Medios de almacenamiento físico:** Derivado de la solicitud para el otorgamiento de usuarios y permisos de acceso a servidores públicos a la plataforma del SENAP, el CFIC integra un expediente físico que se almacena en las instalaciones del Centro Federal de Inteligencia Criminal.
5. Número de titulares en relación con el artículo 32, fracción VI y VIII en el aspecto de cuantitativo de la LGPDPPSO **(ISO 27001)**	FÓRMULA #1 – PARA OBTENER MUESTRA: **X1+X2+X3+Xn… / --- / número total de años = A / número total de años** *X = NÚMERO DE EXPEDIENTES QUE SE TIENEN POR CADA AÑO.* ***A** = TOTAL DE EXPEDIENTES A ANALIZAR* PASO 1: Se suman el número de expedientes que cuentan con titulares de datos personales por año, y se divide entre el número de años totales. **Ejemplo:** Año 2016: 75 expedientes Año 2017: 85 expedientes Año 2018: 34 expedientes Año 2019: 62 expedientes Año 2020: 50 expedientes

SUSTITUCIÓN

75+85+34+62+50 --- **5** (número total de los años sumados)	**306** **= ---** **5**	**= 61.2 (este resultado nos permitirá identificar el año)**

PASO 2: Se localiza un expediente que tenga o se aproxime al número del resultado del paso 1.

Ejemplo:

Resultado **61.2**, el año que más se aproxima es **2019** con un total de 62 expedientes.

Año 2016: 75 expedientes
Año 2017: 85 expedientes
Año 2018: 34 expedientes
Año 2019: 62 expedientes ← Dato más aproximado a **61.2**
Año 2020: 50 expedientes

PASO 3: Una vez ubicado el año del que se tomará la muestra, se procede a verificar que porcentaje es el correspondiente:

- Porcentaje 10% = el número de expedientes sea máximo 500.
- Porcentaje 8% = el número de expedientes sea de 501 hasta 5,000.
- Porcentaje 6% = el número de expedientes sea de 5,001 hasta 50,000.
- Porcentaje 4% = el número de expedientes sea de 50,001 hasta 500,000.
- Porcentaje 1% = el número de expedientes sea mayor a 500,001.

Ejemplo:

Resultado: 61.2, como es un número menor a 500, se utilizará el 10%

61.2 x .10 = 6.12

6.12= 6 expedientes a elegir del año 2019. (C)

C *NÚMERO DE EXPEDIENTES DE LA MUESTRA*

(Cuando el número sea mayor en los decimales a 0.51 se redondea al siguiente número)

PASO 4: En consecuencia, esos 6 expedientes se eligen al azar y se procede a contabilizar **el número de titulares** de datos personales contenidos en cada expediente.

Ejemplo:

Expedientes 3, 13, 23, 33, 43, 53.

Expediente 3: titulares localizados 35
Expediente 13: titulares localizados 72
Expediente 23: titulares localizados 23
Expediente 33: titulares localizados 84
Expediente 43: titulares localizados 9
Expediente 53: titulares localizados 57

TOTAL, DE TITULARES LOCALIZADOS EN LOS EXPEDIENTES MUESTRA:
35+72+23+84+9+57 = 280

B *= TOTAL DE LOS TITULARES LOCALIZADOS EN NUESTROS EXPEDIENTES MUESTRA*

FÒRMULA #2 - TOTAL DE TITULARES DE TODOS LOS AÑOS:

$$\frac{A \times B}{C} = \text{TOTAL, DE TITULARES}$$

A *= TOTAL DE EXPEDIENTES A ANALIZAR (PASO 1)*

B *= TOTAL DE LOS TITULARES LOCALIZADOS EN NUESTROS EXPEDIENTES MUESTRA (PASO 4)*

C *= NÚMERO DE EXPEDIENTES DE LA MUESTRA (PASO 3)*

SUSTITUCIÓN

$$\frac{85{,}680}{6} = \text{RESULTADO FINAL} = 14{,}280$$

(306X280)/6=Total de titulares

Colocar una tercera fórmula:

<table>
<tr><td></td><td>14,280=Total de titulares

Al final se debe elegir en que rango de los siguientes se encuentra:

EL NÚMERO DE TITULARES:

<500: Datos de hasta 500 personas

<5k: Datos entre 501 hasta 5,000 personas

<50k: Datos entre 5,001 hasta 50,000 personas

<500k: Datos entre 50,001 hasta 500,000 personas

> 500K: Datos de más de 500,000 personas</td></tr>
<tr><td>6. Lista de servidores públicos que tienen acceso al sistema de tratamiento</td><td>
<table>
<tr><th>INSTITUCIÓN</th><th>ROL</th><th>FUNCIONES Y OBLIGACIONES</th></tr>
<tr><td>AIC SUTAI</td><td>Administrador</td><td>Artículo 20, 22 y 23 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia</td></tr>
<tr><td>FGR</td><td>Operador</td><td>Artículo 18 y 19 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia</td></tr>
<tr><td>32 Fiscalías estatales</td><td>Operador</td><td>Artículos 18 y 19 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia</td></tr>
<tr><td>INEGI</td><td>Operador</td><td>Artículo 25 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia</td></tr>
</table>
</td></tr>
</table>

7. En su caso, nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable. **En relación con el artículo 32, fracción V de la LGPDPPSO.**	**NO APLICA.**
8. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican. **En relación con el artículo 32, fracción V de la LGPDPPSO.**	El INEGI podrá acceder a la totalidad de la información de la base de datos del SENAP con el objetivo de verificar que la integración de los datos se realice conforme a la infraestructura de información que establece la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia, así como para dar cumplimiento a lo establecido en el Capítulo V de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia.
9. Ciclo de vida de los datos personales **Inciso D en relación con el artículo 32, fracción V de la LGPDPPSO.**	a) Obtención de los datos personales. La Fiscalía General de la República, las fiscalías y procuradurías de las entidades federativas solicitarán mediante oficio a la STCNPJ el otorgamiento de usuarios y contraseñas, así como los permisos necesarios para que las personas servidoras públicas designadas como responsables puedan acceder a la plataforma del SENAP para la transmisión y validación de información para los fines del cumplimiento a la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia. Los oficios deberán cumplir con los requisitos previstos en el Anexo Técnico del SENAP, tales como: a) Nombre del usuario b) Cargo c) Nivel de acceso d) Marca, modelo y número de serie del equipo e) Dirección IP f) Dirección física (MAC) g) Carta responsiva de confidencialidad h) Perfil solicitado i) Justificación

Aunado a ello, deberán estar acompañados de los compromisos de confidencialidad de cada persona servidora pública para la que se solicite un usuario y contraseña.

El INEGI solicitará mediante oficio a la STCNPJ el otorgamiento de usuarios y contraseñas, así como los permisos necesarios para que las personas servidoras públicas designadas como responsables accedan a la base de datos del SENAP para consultar la información para los fines del cumplimiento a la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia. Los oficios deberán llevar los requisitos enlistados en líneas precedentes, así como los compromisos de confidencialidad de cada persona servidora pública para la que se solicite un usuario y contraseña.

La STCNPJ remitirá al CFIC las solicitudes de usuarios que reciba de parte de las instituciones de procuración de justicia de la Federación y de las entidades federativas, así como los compromisos de confidencialidad suscritos por las personas para las que se soliciten los usuarios y contraseñas, a efecto de que el CFIC autorice los permisos de acceso procedentes, que serán otorgados por la SUTAI, conforme a los mecanismos de seguridad implementados por la UEITICS y con base en el proceso de credencialización establecido en el Anexo Técnico del SENAP.

Los usuarios autorizados de las instituciones de procuración de justicia de la Federación y de las entidades federativas realizarán el proceso de carga masiva de información a la plataforma del SENAP a través de plantillas en formato CSV, que permiten el registro de la información que integran las carpetas de investigación por delitos del fuero común y federal, que incluyen datos confidenciales de las personas víctimas e imputadas, así como sobre el estado procesal de las mismas.

Las plantillas de carga de datos se encuentran definidas de acuerdo con diferentes rubros o entidades de negocio, de tal manera que su organización facilite la generación de las sábanas de información que viajarán al SENAP a partir de una base de datos relacional:

b) Almacenamiento de los datos personales

La STCNPJ conservará una copia digital de las solicitudes de usuarios y de los compromisos de confidencialidad que reciba, que se almacenarán en expedientes digitales en la nube de la FGR.

El CFIC genera un expediente físico que contiene las solicitudes de usuarios de cada institución y los compromisos de confidencialidad, los cuales estarán en resguardado físicamente en las instalaciones del CFIC.

La información estadística se carga y almacena de forma digital, exclusivamente en la plataforma del SENAP, conforme a los parámetros establecidos por el INEGI, y es resguardada por la SUTAI, área responsable de su almacenamiento, hasta ser validada y cargada a la base de datos del SENAP

	La plataforma del SENAP ejecuta un proceso con periodicidad mensual los primeros 10 días hábiles de cada mes, lo que produce el conjunto de información estandarizada en la base de datos del SENAP, la cual estará lista para su consulta por los usuarios autorizados del INEGI, previa autorización por parte de los usuarios acreditados de las instituciones de procuración de justicia de la Federación y de las entidades federativa. c) La infraestructura tecnológica se encontrará ubicada en la nube de la FGR. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen; La información estadística que las instituciones de procuración de justicia de la Federación y de las entidades federativas cargan a la plataforma del SENAP, contiene datos personales con carácter confidencial por lo que sólo podrán transferirse a los usuarios autorizados del INEGI, con el objetivo de que verifiquen que la integración de los datos se realice conforme a la infraestructura de información que establece la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia, así como para dar cumplimiento a lo establecido en el Capítulo V de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia. d) El bloqueo[3] de los datos personales, en su caso, y 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 (Art. 3, fr. IV LGPGPPSO). e) La cancelación, supresión o destrucción de los datos personales. Este proceso se realizará conforme al Catálogo de Disposición Documental de la FGR que le resulte aplicable.
II.	**Funciones y obligaciones de las personas que traten datos personales de conformidad con lo dispuesto en los artículos 18, 19, 20, 23, 24 y 25 de la Norma Técnica**

Roles, funciones y obligaciones en el tratamiento de los datos personales

En relación con el artículo 32, fracción V de la LGPDPPSO.

Los perfiles y niveles de acceso se encuentran definidos en el Anexo Técnico, de conformidad con el artículo 24 de la Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia

Áreas relacionadas	Tratamiento					
	Obtención	Almacenamiento	Uso	Divulgación	Bloqueo	Cancelación
CFIC		X	X	X		
UEITICS		X	X	X		
SUTAI		X	X	X		
UESIER		x	x	x		
Fiscalías y Procuradurías Estatales		x	x	x		
STCNPJ		x	X	x		
INEGI		X	X	X		

III. Análisis de riesgos

1. Requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico

- **Constitución Política de los Estados Unidos Mexicanos**
  Artículo 6°, apartado A, fracción II, que a la letra señala que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

- **Ley del Sistema Nacional de Información Estadística y Geográfica**

Artículo 37, que establece que los datos que proporcionen para fines estadísticos los informantes del Sistema Nacional de Información Estadística y Geográfica (SNIEG) a las Unidades del Estado, serán estrictamente confidenciales y bajo ninguna circunstancia podrán utilizarse para otro fin que no sea el estadístico. El INEGI no deberá proporcionar a persona alguna, los datos referidos para fines fiscales, judiciales, administrativos o de cualquier otra índole.

Artículo 38, que establece que los datos e informes que las personas informantes del SNIEG proporcionen para fines estadísticos y que provengan de registros administrativos, serán manejados observando los principios de confidencialidad y reserva, por lo que no podrán divulgarse en ningún caso en forma nominativa o individualizada, ni harán prueba ante autoridad judicial o administrativa, incluyendo la fiscal, en juicio o fuera de él. Cuando se deba divulgar la información a que se refiere el párrafo anterior, ésta deberá estar agregada de tal manera que no se pueda identificar a los Informantes del Sistema y, en general, a las personas físicas o morales objeto de la información.
Artículo 46, conforme al cual las Unidades del Estado estarán obligadas a respetar la confidencialidad y reserva de los datos que para fines estadísticos proporcionen los Informantes del SNIEG.
Artículo 47, que establece que los datos que proporcionen los informantes del SNIEG, serán confidenciales.
Artículos 103, 104 y 105 que establecen las infracciones imputables a las personas servidoras públicas del INEGI o de las Unidades del Estado, así como artículos 106, 107, 108, 109, 110, 111 y 112 que determinan las sanciones correspondientes.

- **Ley de la Fiscalía General de la República**

  Artículo 97, el cual establece que las bases de datos, sistemas, registros o archivos previstos en la Ley que contengan información relacionada con datos personales o datos provenientes de actos de investigación, recabados como consecuencia del ejercicio de las atribuciones de las personas servidoras públicas de la Fiscalía General o por intercambio de información con otros entes públicos, nacionales o internacionales, podrán tener la calidad de información reservada o confidencial.

- **Ley Federal de Transparencia y Acceso a la Información Pública**

  Artículos 9, 16 y 113, los cuales señalan, en lo general, que los sujetos obligados serán los responsables de los datos personales y de su protección, mismos que no estarán sujetos a temporalidad alguna y sólo podrán tener acceso a estos sus titulares, sus representantes y los Servidores Públicos facultados para ello.

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

  Artículo 31, el cual dispone que 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.

- **Ley General de Responsabilidades Administrativas**

  Artículo 49, fracción V, señala que los servidores públicos incurrirán en falta administrativa cuando sus actos u omisiones incumplan o transgredan la obligación de registrar, integrar, custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o comisión, tenga bajo su responsabilidad, e impedir o evitar su uso, divulgación, sustracción, destrucción, ocultamiento o inutilización indebidos.

- **Código Penal Federal**

  Artículo 225, fracción XXVIII, el cual establece que dar a conocer a quien no tenga derecho, documentos, constancias o información que obren en una carpeta de investigación o en un proceso penal y que, por disposición de la ley o resolución de la autoridad judicial, sean reservados o confidenciales, será considerado un delito.

- **Código Nacional de Procedimientos Penales**

  Artículo 106, el cual señala la reserva sobre la identidad, la cual, en ningún caso, se podrá hacer referencia o comunicar a terceros no legitimados la información confidencial relativa a los datos personales de los sujetos del procedimiento penal o de cualquier persona relacionada o mencionada en éste. Toda violación al deber de reserva por parte de los servidores públicos será sancionada.

- **Política para la Gestión de la Confidencialidad en la Información Estadística y Geográfica.**

  Artículo 4 establece que, en materia de confidencialidad estadística, se debe evitar la identificación directa o indirecta de las personas informantes del SNIEG y, en general, de las personas físicas o morales objeto de la información, y se debe evitar que los datos proporcionados por las personas informantes del SNIEG se usen para fines que no sean los estadísticos.
  Artículo 7 establece que los datos que proporcionen las personas informantes del SNIEG a las Unidades del Estado serán estrictamente confidenciales y bajo ninguna circunstancia podrán utilizarse para otro fin que no sea el estadístico, ni se deberán proporcionar a persona alguna para fines fiscales, judiciales, administrativos o de cualquier otra índole, de acuerdo con lo establecido en el artículo 37 de la Ley del SNIEG.
  Artículo 8 establece que los datos e informes que las personas informantes del SNIEG proporcionen para fines estadísticos y que provengan de registros administrativos no harán prueba ante autoridad judicial o administrativa, incluyendo la fiscal, en juicio o fuera de él, de acuerdo con lo establecido en el artículo 38 de la Ley del SNIEG.
  Artículos 10 y 11 establecen las acciones que, en la producción de información estadística y geográfica, las Unidades del Estado deberán realizar para garantizar la confidencialidad por diseño y evitar la identificación directa e indirecta de las personas informantes del SNIEG y, en general, de las personas físicas o morales objeto de la información, entre las que se destaca el deber de evaluar el riesgo de identificación, de acuerdo con la clasificación prevista por el artículo 11, fracción V, incisos a), b), c) y d).
  Artículos 12 que establece que, cuando el riesgo de identificación sea alto o medio, las Unidades del Estado no deberán difundir la Información, o bien deberán analizar la viabilidad de difundir la Información en forma diferente, de manera que el nivel de riesgo de Identificación sea bajo o nulo.
  Artículo 13 que enumera las posibles estrategias de anonimización que las Unidades del Estado deberán implementar para reducir el riesgo de identificación directa o indirecta de las personas informantes del SNIEG y, en general, de las personas físicas o morales objeto de la información.
  Artículo 14 que establece que las Unidades del Estado deben asegurarse, mediante el análisis y evaluación, de que previo a la difusión, la información estadística georreferenciada y/o geocodificada no contenga identificadores o datos confidenciales que pudieran facilitar la Identificación directa o

	indirecta de las personas informantes del SNIEG y, en general, de las personas físicas o morales objeto de la información. Artículo 16 que establece que las Unidades del Estado deberán realizar revisiones de confidencialidad en la producción de información estadística y geográfica por lo menos una vez al año con el objetivo de identificar situaciones que aumenten el riesgo de que una persona física o moral objeto de la información sea identificada. Cuando se detecten vulnerabilidades se deberán implementar mecanismos para corregirlas y en todos los casos deberá enviarse el informe al Instituto. Artículo 17 que enumera las medidas que las Unidades del Estado deberán verificar en materia de tecnologías de la información y comunicaciones para garantizar la confidencialidad de los datos personales que se recaban con fines estadísticos. • **Norma Técnica para la Producción de Información del Sistema Estadístico Nacional de Procuración de Justicia.** Artículo 23. La seguridad de la información de la base de datos estará a cargo de la Fiscalía General de la República, a través de la Agencia de Investigación Criminal, la cual tendrá a su cargo el almacenamiento de los datos y deberá garantizar la implementación de las medidas y mecanismos de seguridad necesarios para el resguardo, protección, confidencialidad y cuidado de la información, para lo cual emitirá el documento de seguridad correspondiente, apegándose a la Política para la Gestión de la Confidencialidad en la Información Estadística y Geográfica. • **Código de Ética de las Personas Servidoras Públicas de la Fiscalía General de la República.** Artículo 7, inciso u, el cual establece que las personas servidoras públicas en el ejercicio de sus funciones privilegiarán el principio de máxima publicidad de la información pública, por lo que deben permitir y garantizar el acceso a la información, sin más límite que el que imponga el interés público y los derechos de privacidad de las y los particulares, atendiendo con diligencia los requerimientos de acceso y proporcionando la documentación que generen, obtengan, adquieran, transformen o conserven; y en el ámbito de su competencia, difundirán de manera proactiva información gubernamental, como un elemento que genera valor a la sociedad y promueve un gobierno abierto, protegiendo los datos personales que estén bajo su custodia.
2. El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida	La obtención y tratamiento de datos personales, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos en término de lo que dispone ésta ley; lo anterior, en virtud de que la Fiscalía General de la República es un sujeto obligado competente en instancia de seguridad, procuración y administración de justicia, por lo que se cuenta con medidas de seguridad de nivel **alto**, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

3. El valor y exposición de los activos involucrados en el tratamiento de los datos personales	Activo	Amenaza	Medida de seguridad existente	Daño/Impacto	Potencial / Probabilidad
	Azure SQL Database Managed Instance	Accesos no autorizados, Software malicioso.	Se cuenta con un WAF (Firewall de Aplicaciones Web), el cual ofrece una protección centralizada de la aplicación. Autentificación mediante usuario y contraseña para ingresar a la instancia SQL. Microsoft Entra ID para la autorización de acceso a la base de datos Azure SQL. Asignación de roles en la base de datos para administrar los privilegios de usuarios a nivel técnico.	Pérdida parcial de la información	**Poco probable**
	Azure Blob Storage	Accesos no autorizados, Software malicioso.	Se cuenta con un WAF(Firewall de Aplicaciones Web), el cual ofrece una protección centralizada de la aplicación.	Perdida parcial de la información	**Poco probable**

			Microsoft Entra ID para la autorización del acceso a los datos de blobs Claves mediante tokens SAS		
	Sistema Operativo de los Equipos de cómputo (archivos con bases de datos)	Virus	Se utiliza un antivirus.	Pérdida total o parcial de la información	**Poco probable**
	Archivo electrónico de almacenamiento	Daño en carpetas compartidas y de resguardo personal	Se hace un resguardo de la información en los equipos de cómputo de los analistas de información involucrados	Pérdida total o parcial de la información	**Poco probable**
	Sistemas de obtención de Información (sistemas institucionales)	-Hackeos -Perdida de usuarios y contraseñas	-Red de internet Segura	Robo y extracción de información	**Poco probable**
	Equipo de cómputo (Equipo físico)	- Mantenimiento insuficiente - Susceptibilidad de daño físico	El resguardo y cuidado de los equipos es responsabilidad del analista al que fue asignado	Pérdida total o parcial de la información.	**Poco probable**
	Suministro eléctrico de alimentación al	Variaciones en suministro eléctrico	Se cuenta con dispositivos reguladores de voltaje	Pérdida total o parcial de la información.	**Poco probable**

	Equipo de cómputo				
	Expedientes, archivos y documentos físicos	Deterioro causado por el paso del tiempo	Se cuenta con archiveros, mismos que se utilizan para almacenar los expedientes.	Pérdida total o parcial de la información.	**Poco probable**

4. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.

En relación con el artículo 32, fracción IV de la LGPDPPSO.

- **Identificación de personas víctimas o imputadas**

Ocurre cuando las personas informantes del SNIEG y, en general, las personas físicas o morales objeto de la información son identificadas de manera directa o indirecta.

- **Robo de identidad**

Ocurre cuando alguien hurta sus datos personales para cometer fraudes. El ladrón de identidad puede usar esa información para solicitar un crédito, presentar declaraciones de impuestos o conseguir servicios médicos de manera fraudulenta. Estas acciones pueden dañar su buen nombre y su crédito, además de costarle tiempo y dinero para repararlo.

- **Extorsión**

Consiste en obligar a una persona a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o del de un tercero. En la extorsión la delincuencia utiliza la violencia psicológica para intimidar a las víctimas, por ejemplo, utilizando agresiones verbales. En otras ocasiones aprovechan la buena fe de las personas para engañarlas. En la mayoría de los casos, los delincuentes eligen al azar a la víctima, utilizando directorios telefónicos, datos personales obtenidos a través de distintas vías e incluso, tomando la información difundida de forma pública en redes sociales por la propia persona.

- **Secuestro**

Privación de libertad ambulatoria a una persona o grupo de personas, exigiendo, a cambio de su liberación, el cumplimiento de alguna condición, como puede ser el pago de un rescate.

- **Usurpación de funciones**

Se refiere al ejercicio de actos propios de una autoridad o funcionario público. Actos propios de una autoridad o funcionario público son aquellos que están comprendidos categóricamente en la disposición legal o reglamentaria que regula tales actos, y también aquellos que están comprendidos en la línea general o en el contexto de las atribuciones conferidas a la autoridad o funcionario público, sin que sea preciso que lo que se usurpa sea la función específica de un determinado

<table>
<tr><td></td><td>cargo, es decir, basta, por ejemplo, que una persona se presente como policía, sin serlo, y realice actos correspondientes a la policía (detención), sin que sea preciso que se presente como policía judicial. El segundo requisito, esencial, de este delito consiste en atribuirse carácter oficial. Este requisito significa que quien así actúa ha de hacer ver falsamente, con actos capaces, ya sea manifestándolo oralmente, o dándolo a conocer con capacidad bastante para engañar a una persona o colectividad, que se tiene el carácter oficial para ejercer los actos propios de esa autoridad o funcionario público.</td></tr>
<tr><td>5. Evaluación del riesgo de identificación de las personas víctimas o imputadas.

De conformidad con el artículo 11, fracción V, de la Política para la Gestión de la Confidencialidad en la Información Estadística y Geográfica.</td><td>
<table>
<tr><th colspan="4">Nivel de riesgo de identificación inherente a la transmisión de datos personales con fines estadísticos al INEGI.</th></tr>
<tr><th>Riesgo alto.</th><th>Riesgo medio.</th><th>Riesgo bajo.</th><th>Riesgo nulo.</th></tr>
<tr><td>Nombre;
Alias;
CURP;</td><td></td><td>Edad;
Sexo;
Nacionalidad;
Fecha de nacimiento;
Situación conyugal;
Datos de nacimiento;
Residencia habitual;
Lengua extranjera;
Lengua indígena;
Discapacidad;
Alfabetismo o escolaridad;
Ocupación;
Rango de ingresos.</td><td></td></tr>
</table>
</td></tr>
</table>

IV. Análisis de brecha en relación con el artículo 32, fracción III de la LGPDPPSO	
1. Medidas de seguridad existentes y efectivas	**a) Administrativas** • El personal firmó, al ingresar a la institución, una Carta de Confidencialidad en la que acepta estar consciente de la sensibilidad de la información que maneja y de las consecuencias de la divulgación de ésta. • Cláusulas penales. • Código de conducta. • Capacitación en protección de datos personales. **b) Físicas**

	• Acceso al Centro Federal de Inteligencia Criminal exclusivo para el personal, a través de código de barras e identificación de huella dactilar. • Bitácoras y control previo de visitas. • Acceso restringido de teléfonos celulares, dispositivos de almacenamiento externos, unidades de almacenamiento USB y laptops, de forma alternativa se tiene bloqueo de puertos y unidades de lectores de CD'S en los equipos. • Monitoreo de cámaras de vigilancia las 24 horas. **c) Técnicas** • WAF (Firewall de Aplicación Web), servicio de seguridad basado en la nube, el cual ayuda a proteger la aplicación web de vulnerabilidades y ataques cibernéticos. • Se cuenta con un certificado SSL el cual establece una comunicación segura habilita una conexión cifrada hacia la aplicación. • Microsoft Entra ID, es un servicio para proteger y controlar el acceso de cualquier identidad no autorizada hacia la aplicación. • Identity Framework, administrar la autentificación y autorización para el uso de la aplicación. • Se cuenta con medidas de seguridad en la aplicación mediante un usuario y contraseña, lo cual evita que usuarios no autorizados ingresen al sistema. • La aplicación cuenta con distintos roles a fin de asignar los privilegios a los usuarios para permitir el acceso a datos específicos. • Control y asignación de usuarios y contraseñas. • Evitar uso no autorizado a equipos de cómputo, medios de almacenamiento o entorno digital. • Bloqueo y cierre de sesiones. • INTRANET. • Acceso controlado a las cuentas de correo electrónico externo institucional • Para su funcionamiento requiere de parches actualizados del Sistema operativo. • Se cuenta con un certificado de seguridad que debe de ser validado antes de establecer la conexión de la VPN. • El Centro de Computo cuenta con seguridad perimetral (FIREWALL) Conexión segura mediante una VPN.
2. Medidas de seguridad faltantes	**a) Administrativas** • Lineamientos para la seguridad de los datos personales. • Protocolos de borrado seguro de los datos personales. • Protocolo o procedimiento de actuación ante una vulneración a la seguridad de los datos, protocolos de obtención y divulgación de datos personales. • Protocolo de actuación ante daño en carpetas compartidas. • Protocolo de actuación ante información compartida por error. • Protocolo para la creación y acceso a contraseñas y usuarios compartidos. • Capacitación del personal para concientizar de la importancia en el adecuado tratamiento de datos personales. • Capacitación sobre las posibles consecuencias y sanciones en el mal manejo de la información. • Firma de compromisos de confidencialidad por parte de las personas usuarias de la plataforma del SENAP. **b) Físicas**

	• No dejar a la vista documentos con los usuarios y contraseñas de acceso a los equipos y bases de datos. • Protectores de pantalla que no permitan la visualización de esta en ángulos distintos al apropiado para manipular el equipo de cómputo. • Prevención del daño por fenómenos meteorológicos o desastres. • No pegar los usuarios y contraseñas en los equipos de cómputo. • Prevención del daño por fenómenos meteorológicos o desastres. **.c) Técnicas** • Servicio Azure Key Vault, el cual nos permite almacenar información sensible técnica, que pertenecen a la aplicación, es decir; cadenas de conexión, usuario y contraseña de la base de datos y certificados. • Actualizaciones periódicas y constantes del sistema. • Actualización de contraseñas de acceso a los equipos cada tres meses. • No compartir los usuarios y contraseñas de los equipos de cómputo. • Contar con un servidor espejo en alguna Unidad Administrativa de la Fiscalía General de la Republica para resguardo de seguridad. • Evitar el guardado en historial de usuarios y contraseñas. • Reforzar el bloqueo los puertos de acceso de respecto de todas las unidades de almacenamiento. • Implementar copias de seguridad de los servidores para solventar casos de pérdida de información. Mantenimiento a equipos que contienen o almacenan datos personales.
3. Existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.	**a) Administrativas** • Capacitaciones constantes sobre la protección de datos. • Mejor comunicación entre las dependencias para sensibilizar al personal en materia de datos personales, divulgación y uso de la información. **b) Físicas** • Archiveros para el almacenamiento de los expedientes físicos. **c) Técnicas** • Equipos de cómputo más nuevos y sofisticados para el resguardo de la información • Contar con un servidor espejo en alguna Unidad Administrativa de la Fiscalía General de la Republica. Copias de seguridad de toda la información en los servidores para en caso de perdidas poder recuperar dicha información

V. Plan de trabajo				
Acción a implementar	**Meta o resultado esperado**	**Fecha de inicio**	**Fecha de término**	**Indicadores**
Implementar el servicio de Azure Key Vault	Almacenamiento de datos sensibles técnicos de manera segura	Segunda fase del proyecto	Al finalizar la segunda fase del proyecto	Alojar de manera segura las cadenas de conexión, contraseñas y certificados
Monitoreo de cambio de contraseñas	Mitigar o reducir el riesgo de accesos no autorizados		Permanente y se realizará trimestralmente	Certeza de que la contraseña sólo la tiene el usuario

Monitoreo del respaldo de la información de los equipos de cómputo	Retener el riesgo de una pérdida de información		Permanente y se realizará trimestralmente	Certeza de que la información estará almacenada en un lugar seguro y no habrá pérdida alguna de ella
Monitoreo del mantenimiento al software y hardware de los equipos de cómputo	Retener el riesgo de una pérdida de información		Permanente y se realizará trimestralmente	Certeza de que los datos personales estarán protegidos en todo momento
Monitoreo del mantenimiento al mobiliario	Retener el riesgo de una pérdida de información		Permanente y se realizará trimestralmente	Certeza de que los datos personales estarán protegidos en todo momento
Determinar las funciones y roles de captura, validación y explotación de la información para evaluar los posibles riesgos de la información que se maneja en la base de datos	Mitigar o reducir el riesgo de accesos no autorizados		Permanente	Certeza de que los datos personales estarán protegidos en todo momento, Matriz de riesgo
Monitorear la aplicación de la política, protocolos, criterios y mecanismos de seguridad de la información correspondientes a la base de datos	Mitigar o reducir el riesgo de accesos no autorizados. Retener el riesgo de una pérdida de información		Permanente y se realizará trimestralmente	Certeza de que los datos personales estarán protegidos en todo momento
Actualizar el Plan de Trabajo	Mitigar o reducir el riesgo de accesos no autorizados. Retener el riesgo de una pérdida de información		Permanente y se realizará anualmente	Certeza de que los datos personales estarán protegidos en todo momento

VI. Mecanismos de monitoreo y revisión de las medidas de seguridad

Medida de seguridad a monitorear	Medio de verificación	Fecha de inicio	Fecha de término	Responsable
WAF (Firewall de Aplicación Web)	Se lleva a cabo la detección y monitoreo de ataques hacia la aplicación, monitoreo de reglas del firewall, registro de accesos y registro de rendimiento de Azure SQL Database Managed Instance el cual se supervisa en la consola de Azure.	Al inicio del proyecto	Permanente	UEITICS
Certificado SSL	Llevar a cabo el monitoreo de la vigencia del certificado a fin de renovarlo anualmente. Validar que la aplicación	Al inicio del proyecto	Permanente	UEITICS

	cuente con el certificado SSL y no se encuentre abierto el portal hacia el público.			
Microsoft Entra ID	Registros de inicio de sesión de los usuarios que se encuentran autorizados en el servicio de Microsoft Entra ID, mediante sus cuentas de correo electrónico institucional, en caso de no estar dado de alta se deniega el acceso.	Al inicio del proyecto	Permanente	UEITICS
Identity Framework	Registro de autorización por medio de usuario y contraseñ	Al inicio del proyecto	Permanente	SUTAI

	a a través de Identity			
Usuario y contraseña de la aplicación	Registro de la autentificación del usuario para verificar la identidad del usuario a efecto de conceder el acceso a la aplicación, en caso contrario, se deniega el acceso.	Al inicio del proyecto	Permanente	SUTAI
Roles de usuarios	Supervisión de los privilegios asignados a los usuarios mediante roles permitidos hacia la aplicación.	Al inicio del proyecto	Permanente	SUTAI
Solicitar vía oficio a la Dirección competente el cambio de contraseñas de los equipos asignados	Acuse de recibido		Permanente Trimestral	Por definir
Solicitar vía oficio a la dirección competente la última fecha de cambio de contraseñas de los equipos asignados	Acuse de recibido		Permanente Trimestral	Por definir

Solicitar vía oficio a la Dirección competente el estatus del mantenimiento del hardware, software y antivirus de los equipos asignados	Acuse de recibido		Permanente Trimestral	Por definir
Solicitar vía oficio a la dirección competente la actualización del hardware, software y antivirus de los equipos correspondientes y asignados	Acuse de recibido		Permanente Trimestral	Por definir
Solicitar vía oficio a la Dirección competente el mantenimiento del mobiliario asignado	Acuse de recibido		Permanente Trimestral	Por definir
Solicitar vía oficio a la Dirección competente la confirmación del funcionamiento de las medidas de seguridad del Centro correspondientes a la (video vigilancia)	Acuse de recibido		Permanente Trimestral	Por definir
Determinar las funciones y roles de captura, validación y explotación de la información	Reporte de funciones y roles de captura		Permanente Anual	Por definir
Elaborar la documentación del sistema de seguridad correspondiente a la (Política, Manuales, Lineamientos, Criterios, Protocolos y Mecanismos)	Documentos de Seguridad correspondiente a cada sistema		Permanente Anual	Por definir
Elaborar y actualizar la bitácora de seguimiento de los Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad	Registro de acuses y actividades realizadas		Permanente Trimestral	Por definir
Capacitar respecto de las funciones y roles de captura, validación y explotación de la información, así como de la documentación de los sistemas de seguridad	Listas de asistencia		Permanente	Por definir

	Reportes de evaluación de los cursos		Anual	

No obstante, la UETAG, requiere actualizaciones periódicas (6 meses) a los sistemas de tratamiento de datos personales e incluso evaluaciones vinculantes del INAI.

VII. Vulneraciones					
Las vulneraciones previas ocurridas en los sistemas de tratamiento en relación con el artículo 32, fracción VII y VIII en el aspecto de cuantitativo de la LGPDPPSO.	**Vulneración**	**Fecha**	**Motivo**	**Acciones correctivas inmediatas**	**Acciones preventivas implementadas (futuro)**
	NO HA OCURRIDO NINGUNA VULNERACIÓN				