POLÍTICAS DE SEGURIDAD EN LOS SISTEMAS DE DATOS PERSONALES DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA.

DIRECCIÓN GENERAL DE ADMINISTRACIÓN.

FECHA DE ACTUALIZACIÓN: SEPTIEMBRE 2019.

ÍNDICE:

I. INTRODUCCIÓN. -

De acuerdo con la Constitución Política de los Estados Unidos Mexicanos (CPEUM), el Instituto Nacional de Estadística y Geografía (INEGI), es un organismo con autonomía técnica y de gestión, personalidad jurídica y patrimonio propios, con las facultades necesarias para regular la captación, procesamiento y publicación de la información que se genere y proveer a su observancia.

Es así que, en apego a lo dispuesto por la CPEUM, en su artículo 6º, Base A, fracciones I y ll la información que posea el INEGI es de máxima publicidad, pero la información concerniente a los datos personales será protegida en los términos y excepciones que fijen las leyes, por lo tanto, y de conformidad con lo establecido por los artículos 33 y 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, cuyo objeto es establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados, el INEGI, atiende a los principios de accesibilidad a la información, transparencia, objetividad e independencia, y tiene como obligación, el realizar acciones que coadyuven a identificar y adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal; su adopción es de obligado cumplimiento para las y los Responsables de la Administración de los Sistemas de Datos Personales y, en su caso, de las personas Encargadas del Tratamiento.

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

Es así que, se emite las presentes Políticas sobre el manejo de la Seguridad en los Sistemas de Datos Personales del Instituto Nacional de Estadística y Geografía, en apego a lo dispuesto por los artículos 33, 34, 35 y 36 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los artículos 60, 61 y 62 de los Lineamientos de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Instituto Nacional de Estadística y Geografía, cuya observancia es general y obligatoria para las Unidades y Áreas Administrativas del Instituto y los servidores públicos adscritos a las mismas, para establecer criterios, procedimientos institucionales y responsabilidades de los servidores públicos, a efecto de garantizar el derecho de acceso a la información pública que posee el Instituto, de conformidad con la Ley General de Transparencia y Acceso a la Información Pública, Ley Federal de Transparencia y Acceso a la Información Pública, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y demás disposiciones legales y normativas aplicables.

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

Sabemos que se deben tomar en cuenta los avances tecnológicos, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, es por ello que se adoptan tres niveles de seguridad basados en los

estándares internacionales para la protección de datos personales, los cuales se aplicarán dependiendo del tipo de datos alojados en los Sistemas de Datos Personales.

II. MARCO JURÍDICO-ADMINISTRATIVO. -

a) Constitución Política de los Estados Unidos Mexicanos.

b) Leyes:

b.1. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y
b.2. Ley General de Transparencia y Acceso a la Información Pública.

c) Lineamientos:

c.1. Lineamientos de Transparencia, Acceso y Protección de Datos Personales del Instituto Nacional de Estadística y Geografía.

d) Otras disposiciones:

d.1 Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/83122/MODELOS_Y_GU_AS_17.pdf

III. OBJETO. -

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

IV. ÁMBITO DE APLICACIÓN. -

El presente documento será de aplicación obligatoria a las y los servidores públicos del INEGI responsables de la Administración de los Sistemas de Datos que contienen datos de carácter personal, así como a las personas externas cuyos servicios contratados por el INEGI, estén relacionados con el uso de dichos sistemas.

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

a. Las personas responsables, encargadas y usuarias de los Sistemas de Datos Personales en el INEGI;
b. El Comité de Transparencia del INEGI, y
c. La Coordinación General de Informática del INEGI.

Todo el personal del INEGI que tengan acceso a los datos personales, está obligado a conocer y aplicar las medidas de seguridad propias de cada Sistema en el que se concentren los datos y es aplicable en todas y cada una de las fases del tratamiento de los datos personales, iniciando desde la obtención de los mismos y finalizando con su cancelación en los Sistemas.

V.- DISPOSICIONES GENERALES.

5.1 NIVELES DE SEGURIDAD. -

Los niveles de seguridad, se identificarán por cada Responsable de la Administración de los Sistema de Datos que contienen datos de carácter personal, considerando los estándares Internacionales de Seguridad Aplicables y las Recomendaciones sobre medidas de seguridad aplicables a los Sistemas de Datos Personales[1].

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

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

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

A.- NIVEL BÁSICO

Las medidas de seguridad marcadas con nivel básico serán aplicables a todos los Sistemas de Datos Personales.

Se considerarán aplicables las medidas de seguridad de NIVEL BÁSICO a los Sistemas de Datos Personales que contengan algunos datos que enseguida se mencionan:

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

[1] Ver inciso II de las *Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales. Disponible en:* https://www.gob.mx/cms/uploads/attachment/file/83122/MODELOS_Y_GU_AS_17.pdf

B. NIVEL MEDIO

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

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

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

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

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

C. NIVEL ALTO

Los Sistemas de Datos Personales que contengan alguno de los datos personales sensibles que se enlistan a continuación, además de cumplir con las medidas de seguridad de nivel básico y medio, deberán tomar las marcadas con nivel alto.

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

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

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

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

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

c.6. **ORIGEN:** Étnico o racial.

VI.- GLOSARIO. -

1. **Administrador del Sistema:** El personal del INEGI que tiene a su cargo la responsabilidad de la administración del sistema y de los operadores.

2. **Área de consulta de Datos Personales:** El espacio destinado para que el personal autorizado examine aquellos datos personales que estén autorizados a consultar, sin posibilidad de modificar su contenido.

3. **Área de recepción de Datos Personales:** El espacio donde se reciben datos personales en cualquier tipo de soporte (físico, electrónico o ambos) en tanto se sigan las demás fases de su tratamiento para integrarlos a uno o más Sistemas de Datos Personales.

4. **Área de resguardo de Datos Personales:** El espacio para almacenar datos personales que han recibido el tratamiento correspondiente para que formen parte integral de uno o más Sistemas de Datos Personales, sin importar el soporte (físico, electrónico, o ambos) utilizado para su almacenamiento.

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

6. **Centro de Datos**: Espacio físicos donde se concentran la Infraestructura Tecnológica principal y los Recursos de TIC necesarios para procesar, transmitir, almacenar, resguardar y respaldar la Información Electrónica institucional.

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

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

9. **Divulgación de incidentes:** Las acciones que adoptan el Titular del Área y el Responsable de los Sistemas de Datos Personales, a efecto de dar a conocer a las Autoridades competentes, a los titulares de los datos y, en su caso, al público en general los actos deliberados (intrusión, robo, etc.), los acontecimientos de caso fortuito o de fuerza mayor (desastres naturales, incendios, huelgas, etc) que hubieren ocasionado la pérdida total o parcial de los datos personales bajo su custodia.

10. **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

11. **Encargado:** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable.

12. **Instituto o INEGI**: Instituto Nacional de Estadística y Geografía.

13. **Intrusión:** Acción que una o más personas realizan para introducirse, sin derecho, en uno o más Sistemas de Datos Personales, a fin de alterar, copiar o sustraer datos personales que formen parte de esos sistemas.

14. **Malware:** Software malicioso o maligno utilizado por personas para causar daños en una o más computadoras o para sustraer archivos de los equipos; es decir, virus, gusanos cibernéticos, “caballos de Troya”, “Spyware”, “bots”, y “rootkits”, y los que se creen posteriormente con el mismo propósito.

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

16. **LTAIPDPINEGI:** Lineamientos de Transparencia, Acceso a la Información y Protección de Datos Personales del Instituto Nacional de Estadística y Geografía.

17. **Personal de sistemas:** El personal que labora en el área de tecnologías de información.

18. **Plan de respaldo**: documento que refiere los tipos de respaldo de información y su periodicidad que se deben realizar para un Sistema informático desarrollado.

19. **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, en el caso particular el INEGI.

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

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

22. **Sistema informático**: Conjunto de algoritmos y procedimientos que conforman aplicaciones o programas de cómputo que permiten procesar y almacenar datos bajo requerimientos definidos para cubrir alguna necesidad específica.

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

24. **Tratamiento de datos personales:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

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

VII.- ESPECIFICACIONES TÉCNICAS.

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

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, las Unidades o Áreas Administrativas del INEGI deberán elaborar un Inventario de los Sistemas de Datos Personales y de los Sistemas de Tratamiento.

INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO (ANEXO 1) Arts. 33, fracc. III y 35 de la LGPDPPSO; Art. 60 de los LTAPDPINEGI.							
Unidad Administrativa	Nombre del Sistema	Responsable del Sistema		Tipo de Datos Personales contenidos en el Sistema	Nivel de Seguridad	Uso que se le da al Sistema	Objeto del Sistema
		Nombre	Cargo				

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

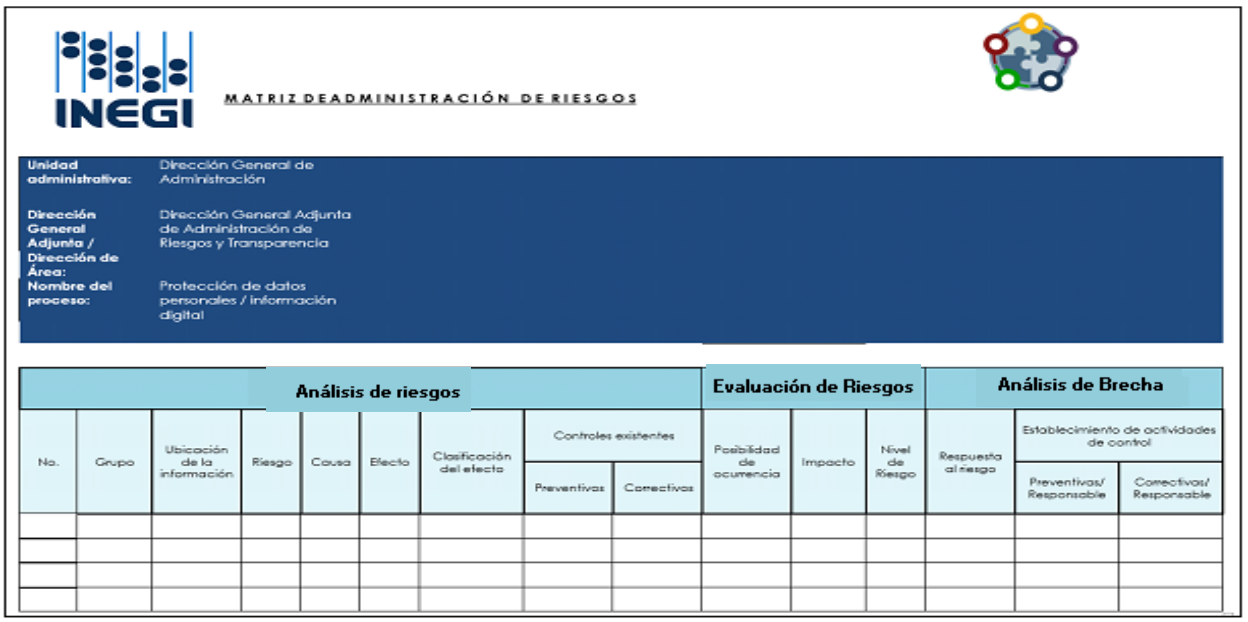
Para establecer y mantener las medidas de seguridad para la protección de los Sistemas de Datos Personales, las Unidades o Áreas Administrativas del INEGI deberán definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Anexo 2) Arts. 33, fracc. II y 35, fracc. II de la LGPDPPSO; Arts. 61 y 62 de los LTAPDPINEGI.						
Artículo 35, Fracción II…						
II. Las funciones y obligaciones de las personas que traten datos personales; **Objetivo: Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;**						
	Unidad Administrativa	**Responsable del Sistema**	**Cargo**	**Nombre del Sistema de Tratamiento de Datos Personales**	**Funciones**	**Obligaciones**
1						

7.3 MATRIZ DE RIESGOS Y ANÁLISIS DE BRECHA.

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

Formato de Matriz de Riesgos y Análisis de Brecha que deberán requisitar todas las Unidades o Áreas Administrativas que mantienen y operan Sistemas de Datos Personales.



INEGI

MATRIZ DEADMINISTRACIÓN DE RIESGOS

Unidad administrativa:	Dirección General de Administración
Dirección General Adjunta / Dirección de Área:	Dirección General Adjunta de Administración de Riesgos y Transparencia
Nombre del proceso:	Protección de datos personales / Información digital

Análisis de riesgos									Evaluación de Riesgos			Análisis de Brecha		
No.	Grupo	Ubicación de la información	Riesgo	Causa	Efecto	Clasificación del efecto	Controles existentes		Posibilidad de ocurrencia	Impacto	Nivel de Riesgo	Respuesta al riesgo	Establecimiento de actividades de control	
							Preventivas	Correctivas					Preventivas/ Responsable	Correctivas/ Responsable

7.4 PLAN DE TRABAJO.

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

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

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Anexo 4) Arts. 33, fracc. VI y 35, fracc. V de la LGPDPPSO; Arts. 61 y 62 de los LTAPDPINEGI.	
Plan de Trabajo	
Medidas de seguridad faltantes	**Actividades por desarrollar**

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

En cumplimiento a lo que establecen los artículos 33, fracción VII y 35, fracción VI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y los artículos 61 y 62 de los Lineamientos de Transparencia, Acceso y Protección de Datos Personales del Instituto Nacional de Estadística y Geografía; y con el objeto de establecer y mantener las medidas de seguridad para la protección de los Sistemas de Datos Personales, las Unidades o Áreas Administrativas del INEGI deberán monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

En éste contexto, es importante señalar la diferencia entre un soporte físico y un soporte electrónico, debido a que las medias de seguridad que el Titular de la Unidad Administrativa o Área responsable implemente para cada Sistema de Datos Personales, están estrechamente relacionadas con el tipo de soportes utilizados.

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

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

Con independencia del tipo de sistema en el que se encuentren los Datos Personales o el tipo de tratamiento que se efectúe, el personal titular de la Unidad Administrativa o Área responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico; en estas últimas, coadyuvando para tal efecto con la Coordinación General de Informática para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, debiendo solicitar para ello la intervención de la Coordinación General de Informática en ejercicio de las atribuciones que le confiere el Reglamento Interior del Instituto Nacional de Estadística y Geografía.

Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales que implementen las Unidades y Áreas Administrativas responsables de Sistemas de Datos Personales deberán estar documentadas y contenidas en el Sistema de que se trate, en términos de lo dispuesto por la Ley General de Protección de Datos en Posesión de Sujetos Obligados, los Lineamientos de Transparencia, Acceso y Protección de Datos Personales del Instituto Nacional de Estadística y Geografía y demás disposiciones administrativas aplicables.

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

7.6.1 ACCESO Y CONSULTA DE DATOS PERSONALES.

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

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

- Deberá darse a conocer al personal del INEGI y personal externo a los que se les proporcione el acceso a los Sistemas de Datos Personales, las situaciones que son consideradas como uso inadecuado, así como de las consecuencias de incurrir en alguna de ellas.

- Deberán establecerse medidas de control de acceso físico y lógico para reducir la probabilidad de que los Sistemas de Datos Personales sean accedidos por personal no autorizado, dichos controles deberán cumplir con los requisitos de seguridad propios del tipo de información, así como de los requerimientos legales y administrativos correspondientes.

- Las autorizaciones al personal del INEGI y personal externo que por razón de su empleo, cargo o comisión tengan la necesidad de acceder a los Sistemas de Datos Personales, que solicitan permiso para introducir a las zonas de acceso restringido aparatos como computadoras, monitores, pantallas planas laptop o agendas electrónicas, el encargado debe registrar:

    - Nombre del solicitante;
    - Nombre del equipo a introducir;
    - Fecha y hora de la introducción;
    - Razón de la introducción y tiempo que se quedará;

- Fecha y hora de salida del equipo.

- El personal del INEGI responsable de los Sistemas de Datos Personales es el único que autorizará la salida de los soportes físicos y electrónicos, por lo que el encargado registrará el hecho de la siguiente manera:

  - Nombre del solicitante;
  - Nombre de los documentos (físicos o electrónicos);
  - Fecha y hora de salida de documentos;
  - Fecha y hora de devolución de documentos (si aplica);
  - Razón de la salida de documentos.

7.6.2 DIVULGACIÓN DE INCIDENTES.

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

Se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada.

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

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

El personal responsable deberá informar al titular de los datos personales al menos lo siguiente:

I. La naturaleza del incidente;
II. Los datos personales comprometidos;
III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
IV. Las acciones correctivas realizadas de forma inmediata, y
V. Los medios donde puede obtener más información al respecto.

En caso de robo o extravío de datos personales en soportes físicos y/o electrónicos, el personal responsable del o los Sistemas de Datos Personales que corresponda, al tener conocimiento del incidente, dará vista al Órgano Interno de Control y a la Coordinación General de Asuntos Jurídicos para que en uso de facultades presenten en sus respectivas competencias, denuncia o querella en términos a los reglamentos administrativos y legales de acuerdo a sus atribuciones, o determinen lo conducente.

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

7.6.3 SUPERVISIÓN.

De conformidad a lo establecido en el artículo 84, fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales, el Comité de Transparencia habilitará a personal de la Unidad de Transparencia para realizar periódicamente una supervisión conjunta con el Comité del Sistema de Seguridad de la Información, figura encargada de normar los aspectos generales en materia de seguridad de la información; así mismo con la Coordinación General de Informática encargada de proteger desde el ámbito tecnológico la información electrónica institucional, los recursos informáticos y los servicios tecnológicos necesarios para que el INEGI pueda cumplir con las funciones y obligaciones que le corresponda de acuerdo a la normatividad aplicable, así como con las diversas Unidades y Áreas Administrativas que mantienen y operan los Sistemas de Datos Personales, para el cumplimiento de las medidas, controles y acciones previstas en el presente documento, ello independientemente de las medidas adoptadas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

7.6.4 CANCELACIÓN DE DATOS PERSONALES.

Para proceder a la baja o destrucción documental de soportes físicos que contienen datos personales, se observarán las disposiciones en materia de archivos que emita el Instituto Nacional de Estadística y Geografía. Y en su caso, en las Normas para la administración, el registro, afectación, disposición final y baja de bienes muebles del Instituto Nacional de Estadística y Geografía.

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

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

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

- Nombre y firma de la persona que realiza la acción;
- Fecha y hora en que se realiza;

- El destino que se le dará al soporte electrónico desechado;
- Nombre y firma del responsable y del Titular del Área Administrativa correspondiente.

7.6.5. SOPORTES FÍSICOS

A.- ÁREA DE RECEPCIÓN DE DATOS PERSONALES.

- Deberá existir la infraestructura apropiada, mantener en forma organizada y segura los datos personales recibidos en dicha área de recepción y se deberán seguir los procedimientos establecidos para el efecto.

- La recepción de datos personales deberá realizarse en las oficinas de los servidores públicos, cuyas funciones tengan a cargo dicha recepción.

- Al momento de la recepción deberá informarse al titular de los datos personales el objetivo de su recolección.

- El expediente confidencial deberá darse de alta en el Sistema de Datos Personales correspondiente.

- El expediente confidencial deberá resguardarse en el mobiliario identificado, bajo llave, dentro de la oficina del director de área responsable de su resguardo.

- El personal autorizado para la recepción deberá ostentar una identificación visible con fotografía (credencial o Gafete) emitida por el INEGI.

- El personal encargado de los Sistemas de Datos Personales debe actualizar periódicamente los nombres completos y fotografías que se deben exhibir en lugar visible dentro y fuera del área de recepción de datos personales, conforme se vayan presentando cambios de personal.

- No está permitido el libre acceso de personal no autorizado ni de equipo dentro del área de recepción a menos que sea autorizado por el personal Responsable.

- Debe existir señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de recepción.

B.- ÁREA DE RESGUARDO DE DATOS PERSONALES.

- Debe existir la infraestructura apropiada, mantener en forma organizada y segura los datos personales recibidos en dicha área de resguardo en soportes físicos y/o electrónicos.

- De existir ventanas o muros transparentes en el área de resguardo, la visión deberá estar obstruida con material que impida la observación de los datos personales.

- Deben existir las condiciones ambientales idóneas para preservar el estado físico de los documentos que contienen los datos personales durante el tiempo de la conservación.

- La puerta de acceso al área de resguardo debe contar con cerradura, dispositivo electrónico o cualquier tecnología que impida su libre apertura, este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área.

- El mobiliario utilizado dentro del área de resguardo protegerá los datos personales en soportes físicos de condiciones adversas en humedad, temperatura, iluminación solar, polvo, consumo de alimentos y presencia de plagas entre otras.

- El personal autorizado para el área de resguardo, deberá ostentar una identificación visible con fotografía (credencial o Gafete) emitida por el INEGI.

- El personal encargado de los Sistemas de Datos Personales debe actualizar periódicamente los nombres completos y fotografías que se deben exhibir en lugar visible dentro y fuera del área de resguardo de datos personales, conforme se vayan presentando cambios de personal.

- No está permitido el libre acceso de personal no autorizado ni de equipo dentro del área de resguardo.

- Debe existir señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de resguardo.

C.- ÁREA DE CONSULTA DE DATOS PERSONALES.

- Debe existir la infraestructura apropiada y seguir los procesos y procedimientos necesarios de tal manera que sea posible supervisar y vigilar los datos personales en soportes físicos que consultan los responsables de los datos dentro del área de consulta.

- De existir ventanas o muros transparentes en el área de consulta, la visión deberá estar obstruida con material que impida la observación de los datos personales.

- La puerta de acceso al área de consulta debe contar con cerradura, dispositivo electrónico o cualquier tecnología que impida su libre apertura, este mecanismo queda cerrado en horas no hábiles o cuando el personal autorizado que ahí labora abandona el área.

- El personal autorizado para el área de consulta, deberá ostentar una identificación visible con fotografía (credencial o Gafete) emitida por el Instituto.

- El personal del área de consulta debe actualizar periódicamente los nombres completos y fotografías que se deben exhibir en lugar visible dentro y fuera del área de consulta de datos personales, conforme se vayan presentando cambios de personal.

- No está permitido el libre acceso de personal no autorizado ni de equipo dentro del área de consulta, a menos que lo autorice el responsable.

- Debe existir señalización visible sobre las restricciones de acceso, las prohibiciones que aplican y el procedimiento para dar aviso al personal de vigilancia en caso de sospecharse la presencia de personas no autorizadas en el área de consulta.

- Cuando la persona titular de los datos personales requiera el acceso a los mismos, se procederá conforme al procedimiento establecido en el Titulo Tercero de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

7.6.6. SOPORTES ELECTRÓNICOS.

A.- ÁREA DE RECEPCIÓN DE DATOS PERSONALES.

- El equipo de cómputo instalado en el área de recepción debe cumplir con los niveles de seguridad para ser ocupada en zonas de acceso restringido y con el software autorizado por la Coordinación General de Informática.

- El equipo de cómputo deberá estar provisto de la tecnología necesaria y suficiente para verificar la identidad del personal autorizado que labora en el área de recepción. Ello implica que, mediante la verificación de claves de acceso, dicho personal accede al equipo a fin de realizar el tratamiento que corresponda a la recepción de datos personales.

B.- ÁREA DE RESGUARDO DE DATOS PERSONALES.

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

C.- ÁREA DE CONSULTA DE DATOS PERSONALES.

- El personal responsable de la administración de los Sistemas de Datos Personales deberá crear las contraseñas temporales, corroborando su eliminación una vez que se haya terminado el tratamiento de datos personales.

- El personal responsable de la administración de los Sistemas de Datos Personales deberá verificar que el acceso solo se dé a los Titulares de los mismos sin que se tenga posibilidad de modificar o extraer los datos personales, sino solo consultarlos y bajo el procedimiento establecido en el Titulo Tercero de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

- El equipo de cómputo instalado en el área de consulta deberá cumplir con la tecnología y software para equipos de cómputo de áreas restringidas, es decir con clave o contraseñas para que únicamente acceda el usuario identificado para que realice el tratamiento que corresponda al resguardo de datos personales.

D.- PERSONAS AUTORIZADAS Y NO AUTORIZADAS.

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

- El personal responsable, deberá registrar también la asignación, actualización y reemplazo de contraseñas de acceso y demás elementos que entregue a las y los usuarios, para que estos puedan accesar a los Sistemas Informáticos del INEGI, lo anterior, conforme a lo que se establece en los Lineamiento para el Fortalecimiento de la Seguridad de la Información en los Procesos y Servicios Institucionales del INEGI y las Políticas para la Seguridad Informática del INEGI.

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

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

Las siguientes medidas de seguridad de carácter técnico se establecen en concordancia a la normatividad institucional en materia de Tecnologías de Información y Comunicaciones, incluyendo lo establecido en las Políticas para la Seguridad Informática y el Manual de Estándares para el Desarrollo de Sistemas informáticos, su implementación es de carácter obligatorio para los Sistemas de Datos Personales de conformidad con el nivel de seguridad que les corresponda, sin limitar los controles adicionales que puedan derivarse de la elaboración de la matriz de riesgos y del análisis de brecha.

MEDIDAS DE SEGURIDAD DE CARÁCTER TÉCNICO PARA NIVEL BÁSICO.

- Los Sistemas informáticos que se usen de manera compartida por más de un usuario deberán ejecutarse en Servidores de cómputo.

- Los Servidores de cómputo deberán estar resguardados en los centros de datos del Instituto.

- Para facilitar el análisis de las bitácoras, los Servidores de cómputo deberán mantener una sincronización de tiempo bajo el esquema adoptado por el Instituto.

- Los Servidores de cómputo deberán contar con un programa de mantenimiento preventivo.

- Los Servidores de cómputo deberán contar con actualizaciones de seguridad periódicas.

- Los Sistemas informáticos deberán contar con evaluaciones de desempeño y seguridad.

- Los Sistemas informáticos deberán contar con Ambientes de cómputo diferentes al productivo para desarrollo y preproducción.

- Deberán utilizarse cuentas de usuario para delimitar los derechos de acceso a los Sistemas informáticos.

- Deberá llevarse a cabo de manera periódica la revisión de derechos de acceso para las cuentas de usuario.

- Los Sistemas informáticos deberán guardar bitácoras de los accesos, así como cambios a la información.

- Los Sistemas informáticos y bases de datos deberán contar con un Plan de respaldo.

- Se deberá contar con pruebas de recuperación que permitan validar la utilidad de los respaldos.

MEDIDAS DE SEGURIDAD DE CARÁCTER TÉCNICO PARA NIVEL MEDIO.

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

MEDIDAS DE SEGURIDAD DE CARÁCTER TÉCNICO PARA NIVEL ALTO.

Los Sistemas de Datos Personales que contengan datos personales sensibles de conformidad a lo que establecen los artículos 3 fracción X, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2 fracción VII y 56 de los Lineamientos de Transparencia, Acceso a la Información y Protección de Datos Personales del Instituto Nacional de Estadística y Geografía, deberán de cumplir con las medidas de seguridad de nivel básico y medio, además de las derivadas de la matriz de riesgos y análisis de brecha para cada Sistema de Datos Personales.

7.7. PROGRAMA GENERAL DE CAPACITACIÓN.

Con el objeto de establecer y mantener las medidas de seguridad para la protección de los Sistemas de Datos Personales, las Unidades o Áreas Administrativas del INEGI deberán diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Las acciones de capacitación tienen el propósito de que la totalidad del personal del INEGI e integrantes de los sujetos obligados conozcan los aspectos teóricos, conceptuales y normativos fundamentales, en materia de acceso a la información y protección de datos personales.

En este sentido, con el objeto de atender lo dispuesto en la Ley General y Ley Federal, respecto a capacitar y actualizar en forma especializada a los y las servidores(as) públicos(as) en materia de transparencia y acceso a la información pública y datos personales; el INAI proporcionó al INEGI el “Formato del Programa de Capacitación Presencial, Programa de Capacitación con Recursos Propios, Programa de Capacitación en Línea y Programa de Capacitación Especializados”, en donde se requiere informar la cantidad de personal que se capacitará en diversos cursos en materia de transparencia durante el 2019.

Con base a lo anterior, se establece el Programa General de Capacitación, aprobado por el Comité de Transparencia para el ejercicio correspondiente. **(Anexo 5).**

VIII. INTERPRETACIÓN:

La aplicación e interpretación de las presentes Políticas de Seguridad en los Sistemas de Datos Personales del Instituto Nacional de Estadística y Geografía, para efectos administrativos corresponde a la Dirección General de Administración, así como los casos no previstos.

IX. TRANSITORIOS.

ÚNICO. - Las presentes Políticas de Seguridad en los Sistemas de Datos Personales del Instituto Nacional de Estadística y Geografía, entrarán en vigor a partir de su publicación en la Normateca Interna del Instituto.

El presente documento se aprobó en términos del Acuerdo No. CT.001/II OR. /2019, aprobado en la Segunda Sesión Ordinaria de 2019 del Comité de Transparencia, celebrada el 19 de septiembre de dos mil diecinueve.

ACUERDO CT.001/II OR. //2019, de la Segunda Sesión Ordinaria del Comité de Transparencia, por el que se aprueban las Políticas de Seguridad en los Sistemas de Datos Personales del Instituto Nacional de Estadística y Geografía.

X.- ANEXOS.