Defensa
Secretaría de la Defensa Nacional

TREN MAYA
TSÍIMIN K'ÁAK

DOCUMENTO DE SEGURIDAD DE TREN MAYA S.A DE C.V.

2025
Año de
La Mujer
Indígena

DEFINICIÓN

El presente Documento de Seguridad, es un instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas para garantizar la confidencialidad, integridad y disponibilidad de datos personales que resguarda Tren Maya S.A de C.V que se encuentra alineada con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligos, la cual establece como objeto los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de sujetos obligados.

I. INVENTARIO DE DATOS PERSONALES.

A. OBJETIVO.

Documentar todos los Sistemas de Tratamiento físicos y electrónicos donde se efectué tratamiento de datos y se realice una clasificación de todos los datos personales.

B. MARCO LEGAL

a. De conformidad con lo establecido en el artículo 33, fracción III de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece la elaboración de un inventario de datos personales y de los sistemas de tratamiento.

b. Los lineamientos Generales de Protección de Datos Personales para el Sector Público establecen que; el responsable deberá elaborar un inventario de datos personales, considerando al menos los siguientes elementos

1. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales.

2. Las finalidades de cada tratamiento de datos personales.

3. El catálogo de los tipos de datos personales que se traten indicando si son sensibles o no.

4. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales.

5. La lista de servidores públicos que tienen acceso a los sistemas de tratamiento.

6. En su caso, el nombre completo, denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda el responsable.

7. En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que justifican estas.

c. En virtud de lo establecido en el artículo 59 de los Lineamientos Generales, en la elaboración del inventario de datos personales, el responsable deberá considerar el ciclo de vida de los datos personales conforme lo siguiente:

1. La obtención de los Datos Personales.

2. El almacenamiento de los Datos Personales.

3. El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin.

4. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen.

5. El bloqueo de los Datos Personales en su caso.

6. La cancelación, supresión o destrucción de los datos personales.

II. INVENTARIO DE DATOS PERSONALES.

Por lo anterior, Tren Maya S.A de C.V. elaboró los inventarios de los distintos tratamientos de datos personales que realiza identificando los elementos informativos que señala el artículo 58 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público y basados en el ciclo de vida de los datos personales, como lo requiere el artículo 59 de los citados lineamientos. Los inventarios de datos personales pueden ser consultados en el apartado **"Inventarios de Datos Personales"**

III. FUNCIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES.

A. De conformidad con lo establecido en el artículo 3 Fracción XXII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados las personas servidores y servidoras públicas adscritas a las Unidades Administrativas que traten datos personales en el ejercicio de sus funciones en Tren Maya S.A de C.V. deberán observar, cuando menos las medidas de seguridad físicas siguientes:

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.

d. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure sus disponibilidad e integridad.

B. Con fundamento en el artículo 3 Fracción XXIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, las personas servidores y servidoras públicas adscritas a las Unidades Administrativas que traten datos personales en el ejercicio de sus funciones en Tren Maya S.A de C.V deberán observar, cuando menos las medidas de seguridad técnicas siguientes:

a. Prevenir que el acceso a las bases de datos o la información, así como a los recursos, sea por usuarios identificados y autorizados.

b. Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones.

c. Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware.

d. Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de Datos Personales.

C. Adicionalmente, las personas servidoras y servidores públicos de Tren Maya S.A de C.V. al tratar los Datos Personales observarán las siguientes funciones y obligaciones:

a. Funciones:

1. Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.

2. Verificar que el inventario de datos personales y de los sistemas de tratamiento de estos, a los que tienen acceso, se encuentren actualizados.

3. Llevar un registro de los servidores públicos que accedan a los Datos Personales y llevar a cabo las acciones necesarias para que sea necesaria la autenticación de los usuarios.

4. Mantener actualizada la relación de usuarios que traten datos personales.

5. En caso de que se presente algún incidente de vulneración de seguridad de los Datos Personales y de los sistemas de tratamiento de los mismos, informar dicho incidente a la Dirección de Transparencia de Tren Maya S.A de C.V. y llevar el registro de los hechos.

b. Obligaciones:

1. Llevar a cabo permanentemente las medidas de seguridad de carácter administrativo, físico y técnico necesarias para la protección de los datos personales, evitando daño, perdida, alteración, destrucción o uso, acceso o tratamiento no autorizado, así como garantizando la confidencialidad, integridad y disponibilidad de estos.

2. Atender los mecanismos para asegurar que los datos personales a los que tengan acceso en el ejercicio de sus funciones, no se difundan, distribuyan o comercialicen.

D. De conformidad con lo anterior, las funciones y obligaciones del personal de Tren Maya S.A de C.V. que trata datos personales se identificaron de la siguiente manera:

a. A través del Programa de Protección de Datos Personales de la Entidad, en el cual se describen todas las obligaciones que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y los Lineamientos Generales, asociando estas con el área responsable del cumplimiento.

b. A través de los inventarios que se desarrollaron por cada uno de los tratamientos, en los cuales se identificó al personal que realiza el tratamiento, el área al que esta adscrito y la finalidad de dicho tratamiento.

En la siguiente tabla se muestra cómo se identifican las funciones y obligaciones en la y/o Política de Protección de Datos Personales, por cada una de las obligaciones que establece la Ley General y los Lineamientos Generales:

Obligaciones.	**Actividades para su cumplimiento.**	**Unidades Administrativas, responsables del cumplimiento.**	**Medios que facilitan la acreditación del cumplimiento.**
Sujetar el tratamiento de los datos personales a las atribuciones o facultades que la normatividad confiera a Tren Maya S.A de C.V., así como con estricto apego y cumplimiento de lo dispuesto en dicho ordenamiento, los Lineamientos Generales, la legislación que resulte aplicable y en su caso, el derecho internacional, respetando los derechos atribuibles a los particulares	Identificar el marco normativo, que faculta a la Unidad Administrativa a tratar datos personales para cada una de las finalidades y aquel que regula el tratamiento respectivo	Todas las Unidades Administrativas que realicen tratamiento de datos personales.	Marco normativo respectivo

Por su parte, el inventario de datos personales contiene las siguientes columnas, en las cuales se identifican las funciones del personal que interviene en el tratamiento de los datos personales:

Servidores públicos que tienen acceso a las bases de datos personales, así como el área de adscripción.	
Área administrativa:	
Finalidades del acceso de los servidores públicos antes identificados, a las bases de datos personales.	

El Comité de Transparencia a través de la Dirección de Transparencia será el área responsable de dar a conocer al personal adscrito a las Unidades Administrativas de la Entidad el Programa de Protección de Datos Personales, que se basa en un sistema de gestión, a fin de que el personal conozca sus funciones para el cumplimiento del sistema de gestión y las consecuencias de su incumplimiento.

Las funciones y obligaciones del personal que trate datos personales se encuentran definidas en la legislación y normatividad que rige a Tren Maya S.A de C.V., por tanto, para efectos del presente Documento de Seguridad, el marco normativo de referencia se encuentra establecido en el Manual de Organización General del Tren Maya S.A de C.V. publicado en el Diario Oficial de la Federación el veintisiete de septiembre de dos mil veinticuatro.

IV. ANÁLISIS DE RIESGO.

A. En cumplimiento con lo establecido en el artículo 33 Fracción IV de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 60 de los Lineamientos Generales de Protección de datos personales para el sector público, establecen como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización de un análisis de riesgo, como sigue:

B. En virtud de lo establecido en el artículo 60 de los Lineamientos Generales el citado análisis de riesgo de los Datos Personales tratados deberá ser llevado a cabo considerando lo siguiente:

a. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.

b. El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida.

c. El valor y exposición de los activos involucrados en el tratamiento de los datos personales.

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

e. El riesgo inherente a los datos personales tratados.

f. La sensibilidad de los datos personales tratados.

g. El desarrollo tecnológico.

h. Las posibles consecuencias de una vulneración para los titulares.

i. Las transferencias de datos personales que se realicen.

j. El número de titulares.

k. Las vulneraciones previas ocurridas en los sistemas de tratamiento.

l. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

C. De conformidad con lo establecido en el artículo 33 de la Ley General, para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar al menos las siguientes actividades interrelacionadas:

a. Realizar un análisis de riesgo de los datos personales considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser de manera enunciativa mas no limitativa, hardware, software, personal del responsable, entre otros.

b. Con base en lo anterior, el responsable identifica los riesgos derivados del tratamiento de datos personales, es decir, al que están expuestos en cada etapa de su ciclo de vida, para la posterior implementación o adecuación de las medidas de protección o controles, y comprender los impactos de eventos temidos o no deseados.

D. El análisis de riesgos, se encuentra contenido en el **ANEXO "ANÁLISIS DE RIESGOS"**, mismo que se encuentra clasificado como información reservada.

V. ANÁLISIS DE BRECHA

A. El artículo 33, fracción V de la Ley General y 61 de los Lineamientos Generales de protección de datos personales para el sector público, establecen como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización de un análisis de brecha.

   a. Artículo 61 de los Lineamientos Generales: Con relación al artículo 33, fracción V de la Ley General, para la realización del análisis de Brecha el responsable deberá considerar lo siguiente:

      1. Las medidas de seguridad existentes y efectivas.

      2. Las medidas de seguridad faltantes.

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

         Artículo 33 de la Ley General: para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

         Fracción V: Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

      4. El análisis de brecha se encuentra contenido en el **ANEXO "ANÁLISIS DE BRECHA" mismo que se encuentra clasificado como información reservada.**

VI. PLAN DE TRABAJO

A. Los artículos 33, fracción VI y 62 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, establecen como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, la realización de un plan de trabajo como sigue:

   a. Artículo 62 de los Lineamientos Generales: De conformidad con lo dispuesto en el artículo 33, fracción VI de la Ley General, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer. Lo anterior, considerando los recursos designados; el personal interno y externo de su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes.

B. El plan de trabajo se encuentra contenido en el anexo definido "**PLAN DE TRABAJO".** Mismo que se encuentra clasificado como información reservada.

VII. MECANISMOS PARA MONITOREAR Y REVISAR LAS MEDIDAS DE SEGURIDAD IMPLEMENTADAS

A. El artículo 33, fracción VII de la LGPDPPSO establece como una de las actividades a realizar para implementar y mantener medidas de seguridad para la protección de datos personales, el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.

B. El artículo 63 de los Lineamientos Generales establece lo siguiente:

a. Para evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos y, en su caso, implementar mejoras de manera continua el responsable deberá monitorear continuamente los siguiente

1. Los nuevos activos que se incluyan en la gestión de riesgos.
2. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica entre otras.
3. Las nuevas amenazas que podrían estar activas dentro y fuera de la organización y que no han sido valoradas.
4. La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
5. Las vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nievas o pasadas que vuelvan a surgir.
6. El camio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel aceptable de riesgo.
7. Los incidentes y vulneraciones de seguridad ocurridas.

Independientemente de lo anterior el responsable deberá contar con un programa de auditoría, interno o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

De lo anterior es posible identificar que el monitoreo y revisión de las medidas de seguridad tiene el objetivo de fortalecer, a través

de un ciclo de mejora continua, la protección de los datos personales que resguarda este instituto.

A continuación, se desarrollan las acciones de monitoreo y supervisión periódica para las medidas de seguridad de Tren Maya S.A de C.V.

C. Mecanismos de monitoreo.

Para los tratamientos de datos personales de Tren Maya S.A de C.V., se consideran los siguientes tipos de monitoreo:

a. Revisión de cumplimiento de las políticas internas de Tren Maya S.A de C.V., relacionadas con el tratamiento de datos personales. Tiene el objetivo de asegurar que las personas servidoras públicas realicen los tratamientos de datos personales en concordancia con lo dispuesto en la Ley General, los Lineamientos Generales y demás normatividad aplicable en la materia.

   Para ello, cuando se identifica algún cambio en los instrumentos antes mencionados, se deberán realizar las siguientes actividades:

   1. Revisar y, en su caso, actualizar los procesos involucrados en el tratamiento de datos personales.
   2. Revisar y, en su caso, actualizar los avisos de privacidad, las funciones y obligaciones del personal y los inventarios de datos personales, según corresponda.
   3. Evaluar si hubo cambios en las amenazas, vulnerabilidades o impacto de los riesgos relacionados con las modificaciones a la normativa, para actualizar los análisis de riesgos, análisis de brecha y plan de trabajo.
   4. Revisar y, en si caso, adecuar los sistemas de tratamiento para cumplir con los cambios normativos.

b. Revisión del riesgo. Tiene el objetivo de identificar modificaciones a los riesgos identificados en los tratamientos de datos personales, para ellos, se implementan los siguientes monitoreos:

1. Monitoreo del entorno del entorno físico: Para la detección continua de amenazas y vulnerabilidades en el entorno físico, se cuenta con:
   i. Personal de Guardia Nacional para la vigilancia en los accesos a los edificios corporativos y estaciones de Tren Maya S.A de C.V.
   ii. Control de acceso para el personal a través de huella digital o credencial de acceso.
   iii. Control de acceso a través de bitácoras para visitantes y personal de Tren Maya S.A de C.V. que olvidó su credencial.
   iv. Control de acceso a través de bitácoras al personal de Tren Maya que acceda a áreas que manejen información sensible.
   v. Circuito cerrado de cámaras de vigilancia.

2. Actualización del plan de trabajo. Derivado del monitoreo del entorno físico electrónico, se pueden realizar actualizaciones en el plan de trabajo en caso de que se identifiquen cambios en las amenazas, las vulnerabilidades o el impacto de los riesgos identificados. Estos cambios se pondrán a consideración de las áreas encargadas de análisis de riesgos y del Comité de Transparencia.

3. Revisión de avances del plan de trabajo. A través de los mecanismos que se determinen las áreas encargadas del análisis de riesgos, la Coordinación General de TIC´S y el Comité de Transparencia, se hará una revisión de los avancen en el plan de trabajo, identificando las acciones, fechas compromiso y, en su caso, las causas por las cuales no se está cumpliendo el plan de trabajo, para hacer los ajustes correspondientes al mismo.

b. Actualización tecnológica. Cuando se integren nuevos equipos de cómputo, servidores, aplicaciones o tenga lugar una migración tecnológica, se realizará una actualización del análisis de riesgo, análisis de brecha y plan de trabajo.

c. Vulneraciones a la seguridad de los datos personales

1. Las vulneraciones a la seguridad de datos personales se producen cuando la información en posesión de sujetos responsables de su tratamiento sufre un incidente de seguridad que da lugar a la violación de la confidencialidad, disponibilidad o integralidad de los datos.

   De manera enunciativa mas no limitativa se consideran vulneraciones a la seguridad de datos personales las siguientes:

   i. Perdida o destrucción no autorizada de los datos personales en posesión de sujetos que realizan el tratamiento de datos.
   ii. Robo o extravío de los datos personales.
   iii. Uso, acceso o tratamiento no autorizado.
   iv. Daño, alteración, modificación o reproducción no autorizada.
   v. Ataques informáticos de cualquier tipo.

   En el caso de vulneraciones a la seguridad de datos personales, el responsable deberá llevar un registro en que el que se describa, la fecha en la que ocurrió, el motivo de esta y las acciones correctivas implementadas de forma inmediata y definitiva.

   El responsable deberá informar sin demora alguna al titular, y al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, por escrito o por cualquier otro medio que se habilite para tal efecto, las vulneraciones que afecten de manera significativa la información, en cuanto se confirme que esta ocurrió y que el responsable haya empezado a tomar acciones 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.

A. El responsable deberá informar al titular al menos lo siguiente:

i. La naturaleza del incidente.
ii. Los datos personales comprometidos.
iii. Las recomendaciones al titular acerca de las medidas que este pueda adoptar para proteger sus intereses.
iv. Las acciones correctivas realizadas de forma inmediata.
v. Los medios donde pueda obtener más información al respecto.

B. El escrito de notificación al INAI deberá contener la siguiente información.

i. La hora y fecha de la identificación de la vulneración.
ii. La hora y fecha del inicio de la investigación sobre la vulneración.
iii. La naturaleza del incidente o vulneración ocurrida.
iv. La descripción detallada de las circunstancias entorno a la vulneración ocurrida.
v. Las categorías y número aproximado de titulares afectados.
vi. Los sistemas de tratamiento y datos personales comprometidos.
vii. Las acciones correctivas realizadas de forma inmediata.
viii. La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida.
ix. Las recomendaciones dirigidas al titular.
x. El medio puesto a disposición del titular para que pueda obtener más información al respecto.
xi. El nombre completo de las personas designadas y sus datos de contacto, para que puedan proporcionar más información al instituto, en caso de requerirse.

xii. Cualquier otra información y documentación que se considera hacer del conocimiento del instituto.

La Unidad Administrativa responsable del tratamiento de datos personales afectados deberá comunicar al Comité de Transparencia la notificación que haya realizado tanto al titular, como al INAI, el mismo día hábil en que haya realizado las notificaciones respectivas. Lo anterior con la finalidad de elaborar la bitácora correspondiente.

En virtud de lo anterior y con fundamento en el artículo 30 fracción V; 84 fracción V de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 47 segundo párrafo de los Lineamientos Generales de Protección de Datos Personales para el Sector Público que establece que entre los mecanismos que se deberán adoptar para cumplir con el principio de responsabilidad, se encuentra el de establecer un sistema de supervisión que permita comprobar el cumplimiento de las políticas de protección de datos personales; por lo que el Comité de Transparencia será el encargado de ejecuta el mecanismo de monitoreo y supervisión de las medidas de seguridad implementadas en la protección de datos personales a través de los siguientes:

I. Etapa de monitoreo: Tren Maya S.A de C.V. a través del Comité de Transparencia requerirá a cada una de las áreas que reportaron tratamientos de datos personales la elaboración de un reporte en el que deberán precisar:

	Si	No
1. Se han definido, se establecen y mantienen las medidas de seguridad administrativas, técnicas y físicas necesarias para la protección de datos personales		
2. Se ha revisado el marco normativo que regula en lo particular el tratamiento de datos		

	personales en cuestión, a fin de identificar si éste contempla las medidas de seguridad específica o adicional a las previstas en la Ley General y los Lineamiento Generales y se ha definido la procedencia de su implementación		
3.	Se han definido las funciones, obligaciones y cadena de mando de cada servidor público que trata datos personales, por unidad administrativa.		
4.	Se ha comunicado a cada servidor público sus funciones, obligaciones y cadena de mando con relación al tratamiento de datos personales que efectúa.		
5.	Se ha elaborado el inventario de datos personales con los siguientes elementos: • El catálogo de medios físicos y electrónicos a través de los cuales se obtienen datos personales. • Las finalidades de cada tratamiento de datos personales. • El catálogo de los tipos de datos personales que se traten, indicando si son sensibles o no. • El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales. • La lista de servidores públicos que tienen acceso a los sistemas de tratamiento. • En su caso el nombre completo, denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable.		

• En su caso, los destinatarios o terceros receptores de las transferencias que se efectúen, así como las finalidades que las justifican.		
6. En el inventario de datos personales se tomó en cuenta el ciclo de vida de los datos personales, conforme a lo siguiente: • El uso de los datos personales conforme a su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin. • La divulgación de los datos personales considerando las remisiones y transferencia que, en su caso se efectuén; • La cancelación, supresión o destrucción de los datos personales.		
7. Se ha realizado el análisis de riesgo, considerando lo siguiente: • La sensibilidad de los datos personales tratados. • El desarrollo tecnológico. • Las transferencias de datos personales que se realicen. • El número de titulares. • El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados por una tercera persona no autorizada para su posesión.		
8. Se ha realizado el análisis de brecha, tomando en cuenta lo siguiente: • Las medidas de seguridad exostentes y efectivas;		

• Las medidas de seguridad faltantes. • La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o mas controles implementados actualmente.		

Etapa de supervisión. El Comité de Transparencia analizará los reportes de las áreas, verificando aquellos puntos en los que se hubiera reportado "No" como respuesta y se emitirá un dictamen o ficha técnica en el que se plasmarán las recomendaciones o requerimientos que se consideren pertinentes en materia de seguridad, con la finalidad de que las áreas las atiendad y remitan evidencias de su cumplimiento.

VIII. PROGRAMA DE CAPACITACIÓN.

En cumplimiento de lo establecido en la fracción VII del artículo 35 de la Ley General el presente Documento de Seguridad contiene el Programa de Capacitación en materia de Transparencia, Acceso a la Información y Protección de Datos Personales y temas relacionados, con base en las necesidades de capacitación determinadas y con relación a las acciones de capacitación propuestas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

La elaboración del Programa de Capacitación de Tren Maya S.A de C.V., asegura el desarrollo de aptitudes, habilidades y responsabilidades de cada servidor público en materia de transparencia, acceso a la información y protección de datos personales y considera el fortalecimiento de competencia éticas para fomentar en las personas servidoras públicas responsables, la concientización en la importancia y valor social que tiene la transparencia, el acceso a la información, la rendición de cuentas la apertura gubernamental, para fortalecimiento de sociedades y gobiernos democráticos.

En ese sentido el programa de capacitación se divide como a continuación se indica:

Capacitación básica: Dirigida para todas las personas servidoras públicas con nivel de subgerente hasta mando superiores, esto sin perjuicio de poder hacerlo extensivo para el resto del personal que forman la Entidad, abordando los temas siguientes:

- ✓ Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- ✓ Clasificación de la información y Prueba de Daño.
- ✓ Esquema de Mejores Prácticas.
- ✓ Aviso de Privacidad en el Sector Público.

Capacitación especializada: Dirigida para personas servidoras públicas que formen parte del Comité de Transparencia, Gerencia de Protección de Datos Personales, personal designado como enlace de transparencia para el desarrollo e implementación del documento de seguridad, abordando, además de los temas antes listados los siguientes:

- ✓ Sistema de Gestión de Seguridad en Materia de Protección de Datos Personales.
- ✓ Elaboración del Documento de Seguridad.
- ✓ Auditorias Voluntarias en Materia de Protección de Datos Personales en el Sector Público.

IX. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.

El artículo 36 de la Ley General establece la obligación de la actualización del documento de seguridad cuando existan los siguientes eventos:

A. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.

B. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.
C. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración se seguridad ocurrida.

D. Se lleven a cabo acciones correctivas y preventivas ante una vulneración de seguridad.

Es por ello por lo que el Comité de Transparencia deberá estar atento a la actualización de alguno de los supuestos antes señalados, para, en su caso, actualizar el presente documento de seguridad.