ADMINISTRACIÓN DEL SISTEMA PORTUARIO NACIONAL MANZANILLO, S.A. DE C.V.

PROGRAMA DE SEGURIDAD DE DATOS PERSONALES.

Diciembre del 2022

ÍNDICE

Marco Normativo

- Constitución Política de los Estados Unidos Mexicanos, artículo 6, Base A y segundo párrafo del artículo 16.
- Ley General de Transparencia y Acceso a la Información Pública
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
- Ley orgánica de la Administración Pública Federal
- Ley de Entidades Paraestatales
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Lineamientos que establecen los parámetros, modalidades y procesamiento para la portabilidad de datos personales.
- Guía para cumplir con los principios y deberes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

1. Objetivo y alcance del documento.

Identificar los principales elementos en materia de protección de datos personales relacionados con las medidas de seguridad físicas, digitales, administrativas y técnicas, a fin de determinar y salvaguardar las vulnerabilidades, amenazas y riesgos que a nivel general son aplicables a los sistemas de información y áreas físicas en los se manejan datos personales por la Administración del Sistema Portuario Nacional Manzanillo, S.A. de C.V., en adelante (ASIPONA Manzanillo), de conformidad con lo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante LGPDPPSO o Ley) y a los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

El alcance de este documento serán los sistemas de información centralizados y administrados por la Subgerencia de Informática perteneciente a la Gerencia de Planeación, los cuales son utilizados por el resto de las áreas de la ASIPONA Manzanillo, para el manejo y tratamiento de los datos personales, los cuales son responsabilidad de cada una de dichas áreas; asimismo, los espacios físicos en donde se mantienen, operan y resguardan esos datos personales y que son supervisadas por el Área Coordinadora de Archivo.

En este sentido la Administración del Sistema Nacional Portuario Manzanillo, S.A. de C.V., a través de la Subgerencia de Informática y la Coordinación de Archivo en coordinación con la Unidad de Transparencia, en adelante las áreas comisionadas, han elaborado conjuntamente el presente documento de seguridad en observancia de los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de los datos personales, con la intención de brindar homogeneidad en la organización y procesos para la protección de los datos personales.

Por lo anterior, el presente documento tiene como propósito controlar internamente el universo de datos personales en posesión de ASIPONA Manzanillo, el tipo de datos personales que contienen los archivos, los responsables, las obligaciones, el análisis de riesgos y los mecanismos de monitoreo y revisión de las medidas de seguridad, entre otros.

2. Datos personales en posesión de la ASIPONA Manzanillo.

En cumplimiento a lo establecido en los artículos 33, fracción III y 35, fracción I de la Ley General de Datos Personales en Posesión de Sujetos Obligados y 58 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público, la ASIPONA Manzanillo con la finalidad de establecer y mantener las medidas de seguridad para la protección de los datos personales, emitió el presente inventario de datos personales y de los sistemas de tratamiento, con la información básica del tratamiento de datos personales señalado por las Unidades Administrativas de la Institución. **(Anexo 1. Inventario de Datos Personales)**

De los cuales, se mantiene un tratamiento de datos personales desde su obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia, disposición o cualquier otra operación aplicable a ellos, con forme a la normatividad aplicable.

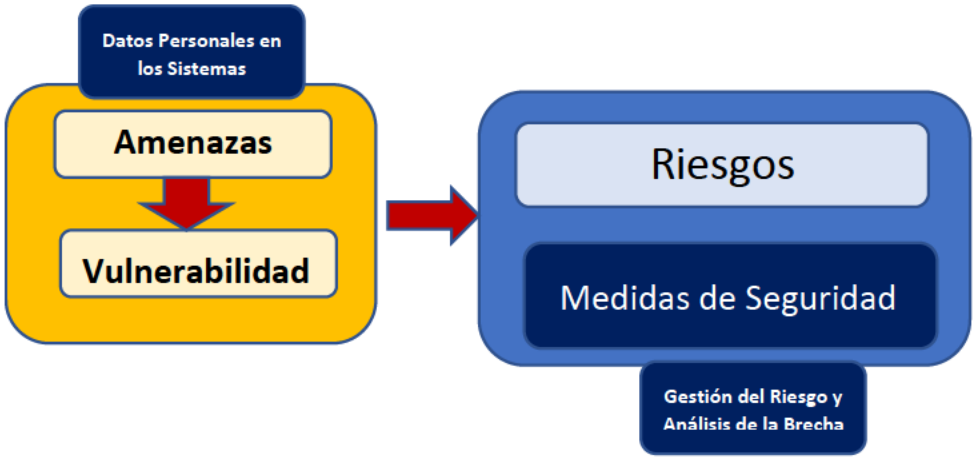
Por lo anterior, la ASIPONA Manzanillo debe establecer políticas, métodos y técnicas orientadas para el tratamiento de esos datos de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley General de Transparencia y Acceso a la Información Pública y Ley General de Archivos. Asimismo, es necesario identificar las vulnerabilidades, amenazas y riesgos a los que se enfrente en esta materia, a fin de poder darles un tratamiento en particular, ya que su importancia se considera crítica y sensible.

Todas las áreas de la ASIPONA Manzanillo que tratan datos personales deben tener conocimiento de sus riesgos y de las medidas de seguridad que deben emplearse para gestionarlos, por lo cual más adelante se presenta tanto el análisis de riesgos como la definición de las medidas tanto físicas como electrónicas o digitales que deberán tenerse en consideración para ello.

3. Medidas de protección generales.

Conforme a la Ley y a las medidas de protección y seguridad que se deben emplear a fin de proteger y salvaguardar los datos personales, las áreas comisionadas, ha identificado las principales vulnerabilidades, amenazas, riesgos y medidas de seguridad generales por medio de las cuales se cubren esos riesgos; asimismo, se ha realizado el análisis de brecha de las medidas de seguridad con las que se cuenta y las que se requieren para gestionar los riesgos.

Las medidas de seguridad requeridas se determinan en base a las vulnerabilidades y amenazas que en conjunto determinan el riesgo, como se muestra a continuación:



El propósito de identificar vulnerabilidades consiste en poder resolver los problemas de seguridad antes de que éstos sucedan, esto significa que debe de ejecutarse bajo un enfoque proactivo y no de manera reactiva; una vulnerabilidad se considera una debilidad en la seguridad de los datos personales; aunque en sí misma no causa daño, puede afectar algún dato cuando se aprovecha o explota por alguna amenaza.

Las vulnerabilidades que podrían existir en relación con la protección de los datos personales se integran en el siguiente listado de debilidades:

1. Protección física de servidores.
2. Protección de bases de datos físicos inadecuados.
3. Controles de acceso físicos inadecuados a los servidores que soportan los sistemas y bases de datos o archivos electrónicos.

4. Controles de acceso físicos inadecuados a los servidores que soportan los archivos físicos.
5. Inadecuada administración y/o mantenimiento de hardware, en el caso de bases de datos electrónicos.
6. Contraseñas débiles o que no se modifiquen periódicamente.
7. Falta de protección en la red a fin de identificar posibles ataques o incidentes de seguridad.
8. Falta de definición de políticas de ciberseguridad.
9. Falta de procedimientos de ciberseguridad que permitan depender del personal que las ejecuta.
10. Carecer de convenios de confidencialidad con el personal interno y externo.
11. Falta de gestión del código fuente de los programas de los sistemas.
12. Acceso de personal del ambiente de desarrollo al de producción y viceversa.
13. Falta de restricción a las cuentas de administración de usuarios y contraseñas.
14. Deficiente o falta de autorización de accesos a los datos personales (mínimo privilegio).
15. Controles de acceso lógicos poco robustos, en el caso de datos localizados en bases electrónicas.
16. Falta de definición de perfiles y roles dentro de los sistemas para delimitar funciones y accesos.
17. Accesos sin requerir una contraseña para autenticar e identificar al usuario, así como nula protección de accesos físicos.

Estas vulnerabilidades podrían ser explotadas por las siguientes amenazas que en conjunto podría potencializar la probabilidad de que ocurran riesgos sobre los datos personales.

La siguiente es una muestra de algunos de los tipos de amenazas intencionales y no intencionales a los que se puede enfrentar la organización, y concretamente, sus activos de información. Las amenazas pueden ser de tipo interno ejecutadas por empleados sobre los datos personales a los que se pretende ganar acceso, desde el interior de las instalaciones de la ASIPONA Manzanillo; o bien pueden ser externas ejecutadas por personal tercero desde localidades ajenas a las la ASIPONA Manzanillo. A continuación, se enlista, de manera enunciativa más no limitativa, el catálogo de las posibles amenazas:

TIPOS DE AMENAZAS	
TIPO	**EJEMPLO**
INTENCIONALES	a) Accesos no autorizados a información o instalaciones; b) Ataque malicioso (físico o lógico); c) Personal interno mal intencionado; d) Personas externas mal intencionado; e) Explotación de vulnerabilidades tecnológicas.
NO INTENCIONALES	a) Desastre natural; b) Falla en el suministro de energía; c) Error, accidente o descuido del personal; d) Falla o descompostura en la infraestructura; e) Demanda excesiva de servicios.

El riesgo de vulneración puede presentarse cuando las amenazas señaladas aprovechen las vulnerabilidades, lo cual deriva en ganar acceso a los datos personales de manera no autorizada con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad por parte de las áreas comisionadas están orientadas a proteger los datos personales.

4. Análisis de riesgos de los datos personales.

Los datos personales que recaba cada una de las áreas que integran la ASIPONA Manzanillo, así como su tratamiento, se rigen por lo dispuesto en la LGPDPPSO y sus Lineamientos, los cuales, al ser un activo relevante, cuentan con medidas de protección que han sido definidas conforme los riesgos que existen en relación a estos, es decir, la identificación de las vulnerabilidades y amenazas a que están sujetos, las cuales en conjunto determinan el nivel de riesgo que se mantiene.

Para evaluar las medidas de seguridad necesarias para proteger los datos personales es necesario la ejecución del análisis de riesgo, de modo que se pueda determinar cuál riesgo es más importante mitigar o los datos que se encuentran más expuestos. Este análisis de riesgos se enfoca en tres variables que afectan la percepción del valor de los datos personales para un atacante:

a) **Beneficio para el atacante.** Aquellos datos personales que representen mayor beneficio tienen más probabilidad de ser atacados (por ejemplo, beneficio económico por venderlos o usarlos).
b) **Accesibilidad para el atacante.** Aquellos datos personales que sean de fácil acceso tienen mayor probabilidad de ser atacados (por ejemplo, miles de personas pueden acceder a la vez a una base de datos a través de un sitio web, pero sólo unas cuantas lo podrían hacer a un archivero), es por ello la trascendencia de los datos que se mantienen de manera electrónica o digital.
c) **Anonimidad del atacante.** Aquellos datos personales cuyo acceso representa mayor anonimidad tienen más probabilidad de ser atacados (por ejemplo, internet es un medio más anónimo que presentarse físicamente a las instalaciones de una institución).

El presente análisis se basa en el inventario de datos personales que se recaban, tratan y resguardan, en las unidades administrativas de la ASIPONA Manzanillo realizado por las áreas y que fue aprobado por el Comité de Transparencia de la ASIPONA Manzanillo, en razón de considerar no solo el dato personal que se recaba o trata como un activo aislado, sino también su relevancia y clasificación en función de las variables anteriores, a fin de ponderar el riesgo e identificar la información que por orden de prioridad requiera tener más protección, y finalmente las medidas de seguridad requeridas y las que hagan falta implementar, lo cual se verá más adelante en “Medidas de seguridad y análisis de brecha”.

Asimismo, a efecto de cumplir con el deber de seguridad, las áreas observarán lo dispuesto en los artículos 32 y 33 de la LGPDPPSO, particularmente de los datos que obran en el inventario aprobado por el Comité de Transparencia.

Del inventario, se ha realizado la estimación de las vulnerabilidades y amenazas que los impactan, así como el nivel de riesgo que esto representa, el cual se determinó en base al tipo de datos y su riesgo inherente y a su nivel de seguridad requerido, como sigue:

a) **Datos con riesgo inherente bajo:** [redacted]

b) **Datos con riesgo inherente medio:** [redacted]

c) **Datos con riesgo inherente alto:** [redacted]

[redacted]

Aunado a lo anterior, para determinar el nivel de riesgo se considera el criterio del riesgo inherente del dato personal, así como el nivel de seguridad requerido para este, en adición a las vulnerabilidades y amenazas, conforme a lo siguiente:

CRITERIOS DEL NIVEL DE RIESGO	
Riesgo Inherente Bajo	Nivel Seguridad Bajo
Riesgo Inherente Medio	Nivel Seguridad Medio
Riesgo Inherente Alto	Nivel Seguridad Alto

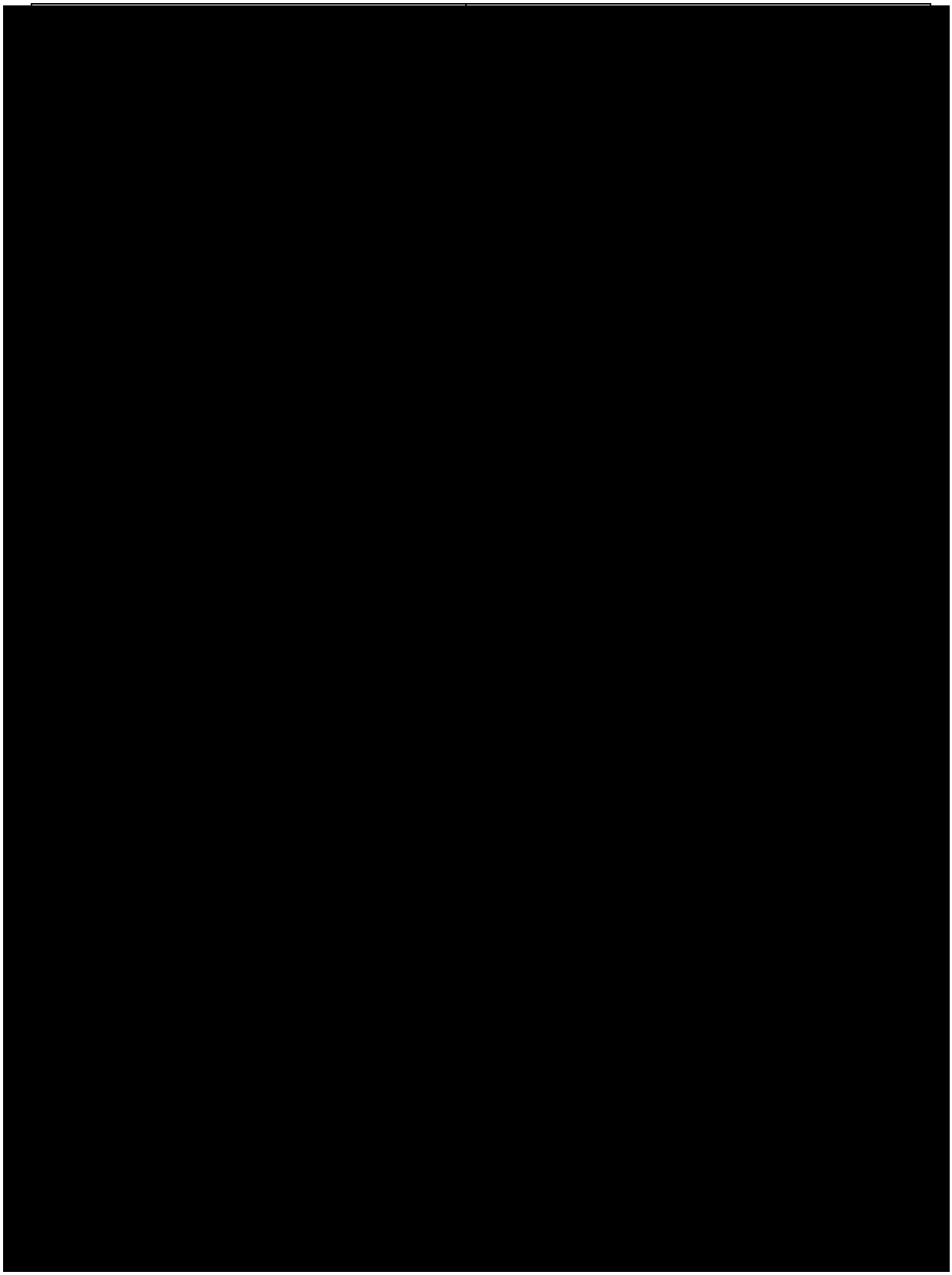
5. Medidas de seguridad y análisis de brecha.

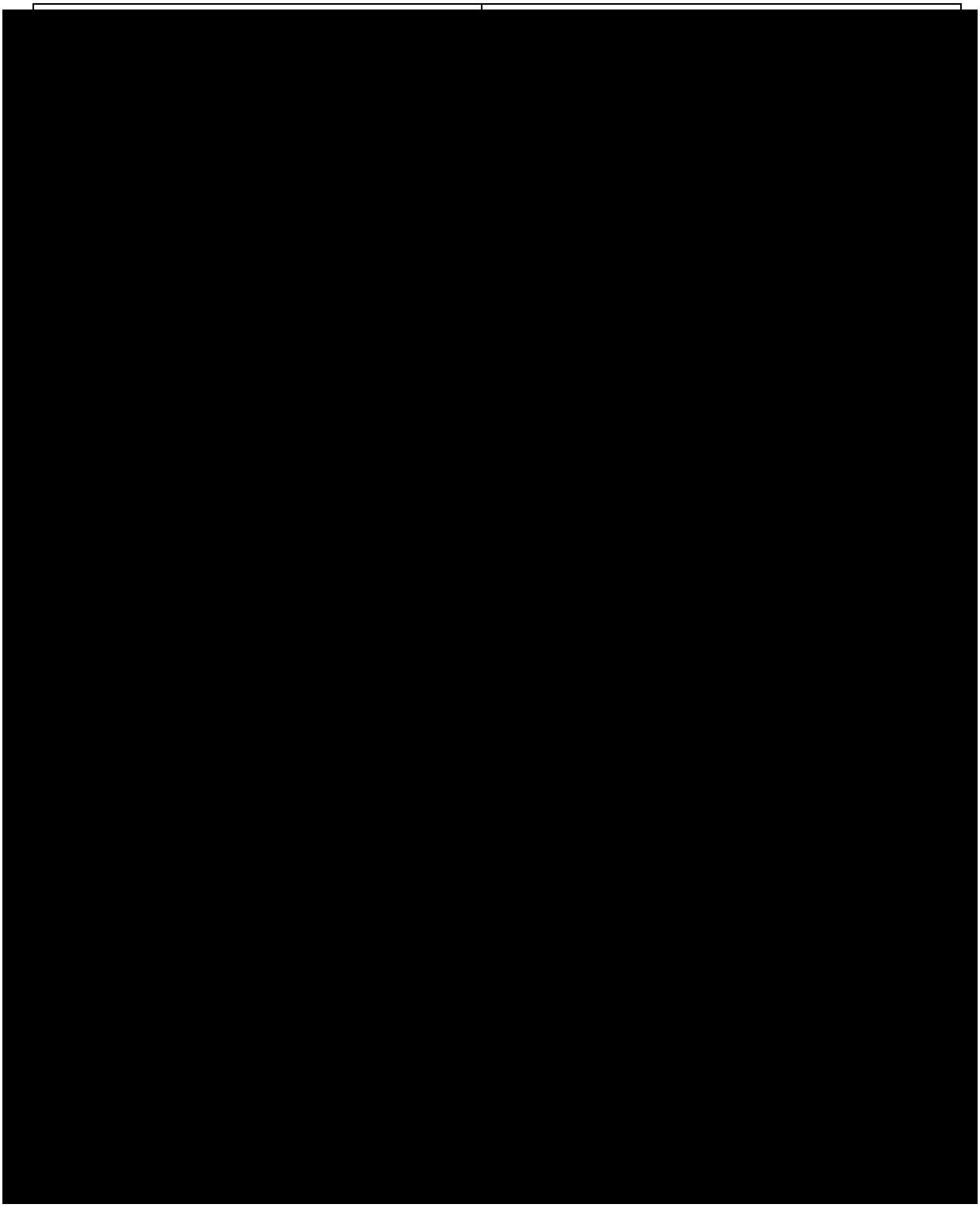
Las medidas de seguridad en materia de tecnología y de seguridad física que se han implementado a fin de mitigar las vulnerabilidades y amenazas descritas, y que representan un mecanismo para cumplir con los objetivos marcados por el artículo 6 de la Ley que son:

1. Proteger los datos personales contra daño, pérdida, destrucción o alteración.
2. Evitar el uso, acceso o tratamiento no autorizado, e
3. Impedir la divulgación no autorizada de datos personales.

Las medidas con las que actualmente se cuenta, así como las requeridas que aún falta por implementar, que en su conjunto integran el análisis de brecha se conforma como sigue:

MEDIDAS DE SEGURIDAD	
Medidas de seguridad existentes	Medidas de seguridad faltantes
[redacted]	



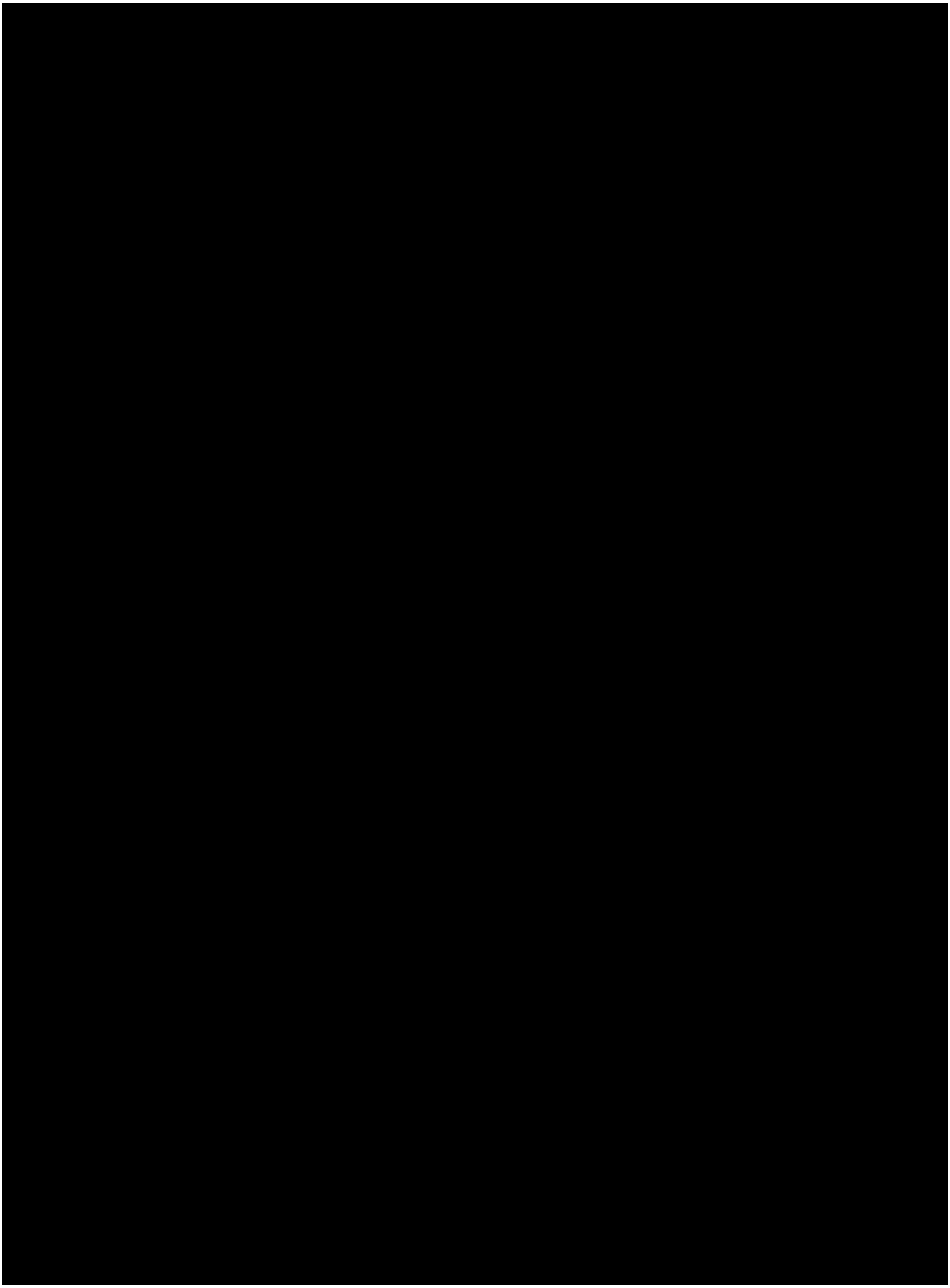


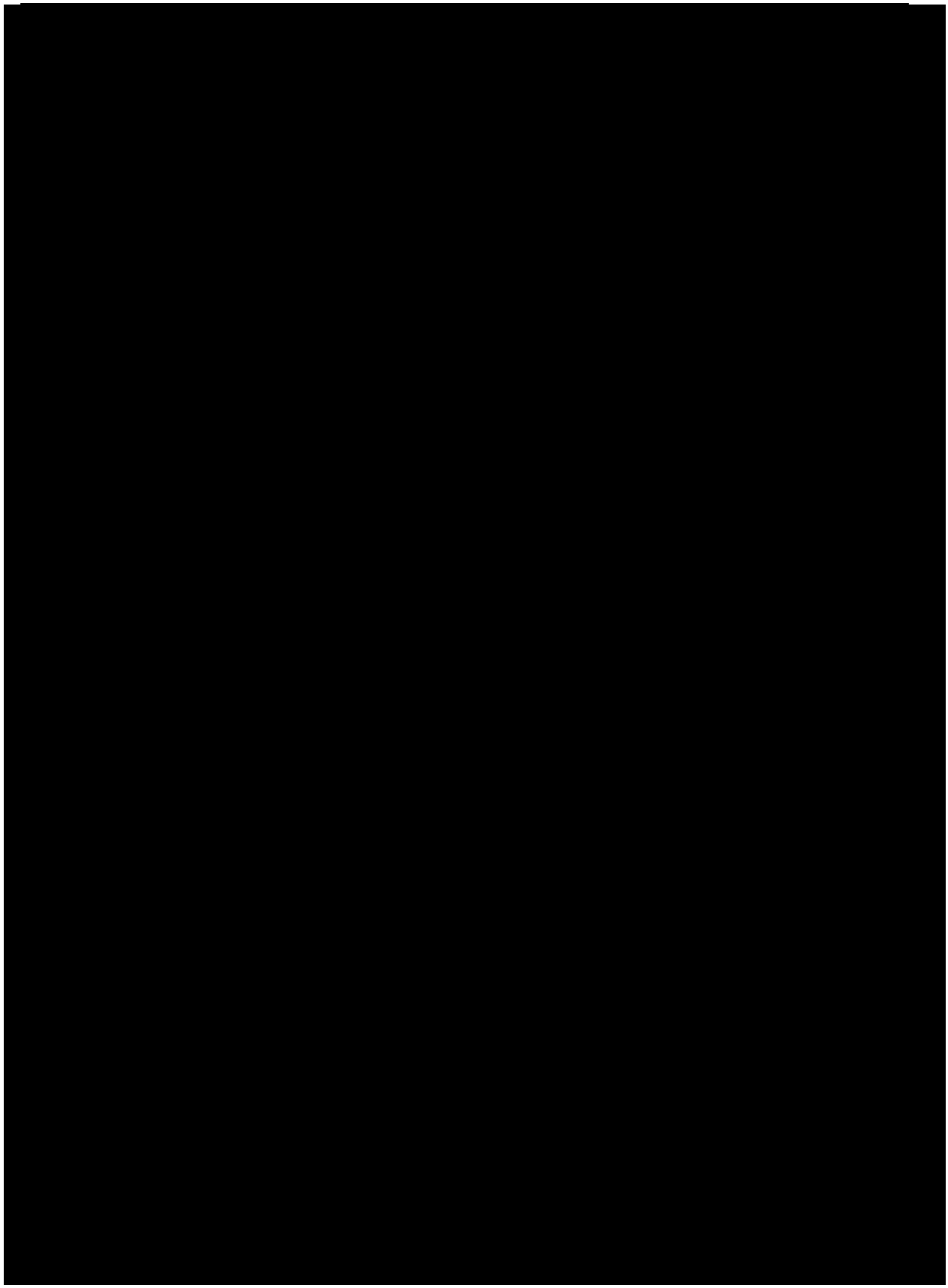
5.1 Monitoreo de las medidas de seguridad.

A fin de supervisar y garantizar el cumplimiento de las medidas de seguridad que se encuentran implementadas en materia de tecnologías de información y

comunicaciones, así como de seguridad física, se han definido controles de monitoreo periódico que permiten el seguimiento de esas medidas, como sigue:

Medidas de seguridad existentes	Mecanismo de monitoreo
[redacted]	



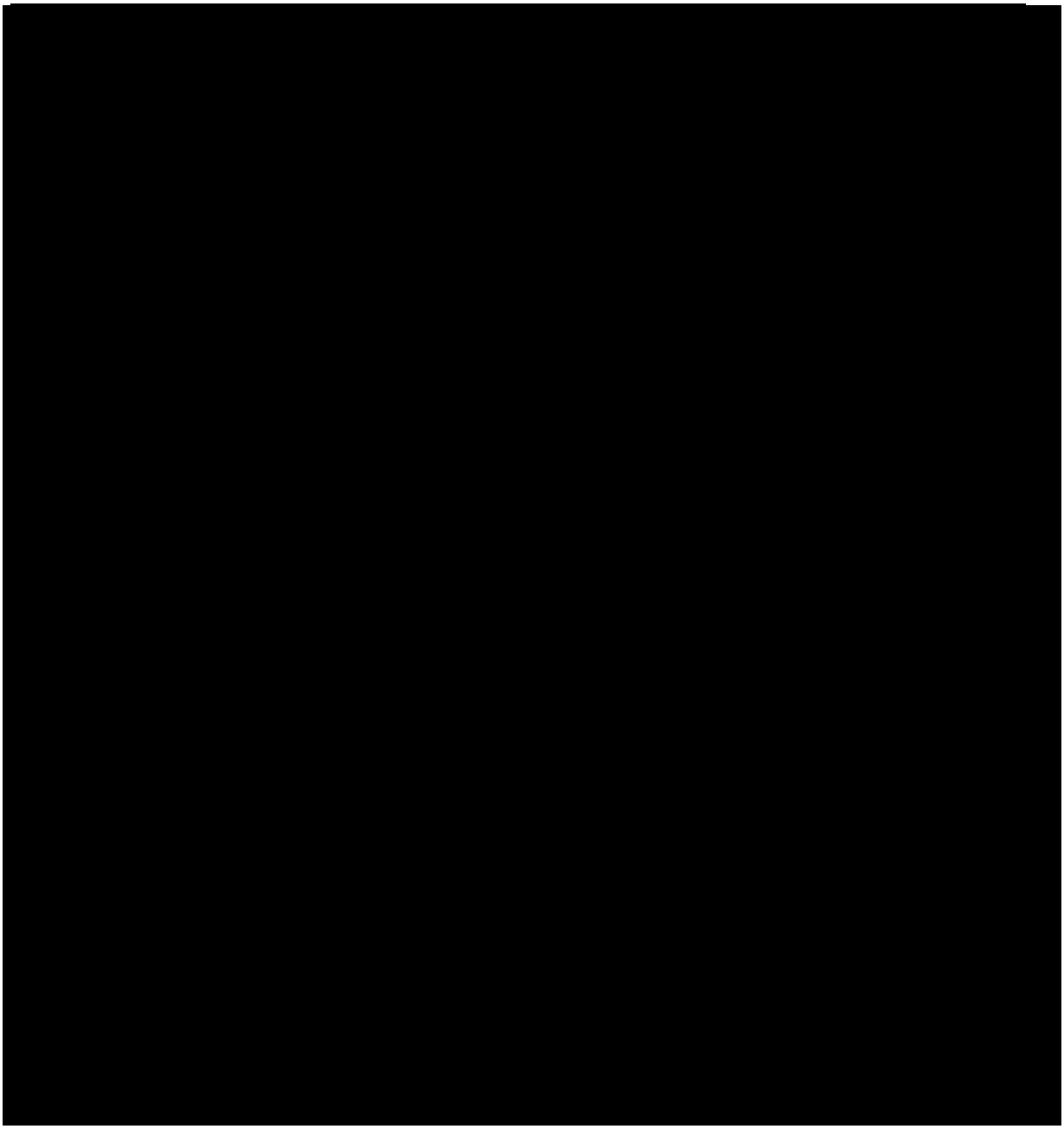


[redacted]

a. Programa de trabajo para la implementación de medidas de seguridad.

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 esas:

Medidas de seguridad faltantes	Actividades por desarrollar.
[redacted]	



6. Políticas de aplicación general en materia de datos personales.

En el ámbito de la seguridad de la información electrónica o digital así como la física, la Subgerencia de Informática y el Área Coordinadora de Archivo en coordinación con la Unidad de Transparencia, han establecido las siguientes políticas de aplicación general para todas las áreas de la ASIPONA Manzanillo, relacionadas con los datos personales que se tratan por medio de sistemas de información, archivos o documentos electrónicos principalmente, correo electrónico, equipos de cómputo, entre otros medios tecnológicos administrados centralmente por la Subgerencia de Informática, así como por las áreas y espacios físicos dentro del alcance del área Coordinadora de Archivo.

6.1 Políticas en Materia de Seguridad de la Información (Tecnología de la Información).

Las siguientes políticas enmarcan los principales rubros de mayor relevancia a considerar, conforme al tratamiento de datos personales y son:

1. Utilizar claves de usuario y contraseñas de usuario de manera exclusivamente personal, así como no compartirlas, prestarlas ni mantenerlas anotadas a la vista de otras personas.

2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que estas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.

3. Notificar de manera inmediata a la Subgerencia de Informática, los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero, a fin de evitar pérdida, robo, eliminación o alteración de información que contenga datos personales, así como asignar una nueva contraseña o clave.

4. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando enviar datos personales o hacerlo asignando una contraseña a fin de procurar su protección.

5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.

6. No difundir, transmitir ni compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.

7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.

8. Procurar solicitar acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio, es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.

9. Triturar todos los documentos físicos que contengan datos personales y ya no sean útiles y/o necesarios para las actividades laborales, así como borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo, los documentos o archivos electrónicos que recaen en esa misma situación, garantizando la completa eliminación de los datos personales que ya no sean necesario de tratar en esos medios.

10. Notificar las bajas de accesos a los sistemas de información de tratamiento de datos personales, con oportunidad, en cuanto sean del conocimiento de los responsables de las áreas, a fin de restringir el acceso a dichos datos por personal no autorizado y que ya no forma parte de la ASIPONA Manzanillo.

6.2 Políticas en Materia de Seguridad Física.

Por otro lado, en el desarrollo de las funciones de seguridad para el tratamiento de datos personales almacenados en archivos físicos, el área Coordinadora de archivo como encargada de la seguridad y resguardo de los inmuebles pertenecientes a la ASIPONA Manzanillo, establece las siguientes políticas son lineamientos obligatorios, que pueden establecer las áreas parlamentarias, técnicas y administrativas:

1. Gestionar la solicitud de préstamo de documentos y/o información mediante memorándum o en su caso, correo electrónico.

2. Solicitar al personal que ingrese al archivo de concentración su registro en la Bitácora principal

3. Concentrar los archivos físicos que contiene datos personales en lugares aislados, preferentemente en las oficinas principales de los titulares de áreas.

4. Procurar solicitar la instalación de chapas con llave a fin de limitar el acceso de personas.

5. Procurar en la medida de lo posible transferir de archivos físicos a bases electrónicas, además de elevar el nivel de seguridad, permitirá la pérdida de información con motivo de amenazas del tipo no intencionales.

6. Limitar el número de personas que tengan acceso a archivos físicos.

7. Realizar un registro interno de personas que ingresan a las oficinas que contienen datos personas en archivos físicos.

8. Procurar suscribir acuerdos de confidencialidad con el personal que maneje datos personales.

9. Reportar inmediatamente al área Coordinadora de archivo de cualquier robo o extravió de documentos que contengan datos personales.

10. Reportar inmediatamente al área Coordinadora de archivo sobre los cambios de personal que manejen archivos físicos que contengan datos personales.

11. Capacitar y sensibilizar al personal de la entidad en materia de Archivos.

7. Propuesta de capacitación en materia de datos personales.

Uno de los factores esenciales para la implementación de los controles y demás medidas de seguridad, la actualización y mejora del inventario de datos personales, el apego a la normatividad y a Ley así como la concientización en la materia de todo el personal involucrado en el tratamiento de datos personales, es el conocimiento y capacitación, por lo que en aprovechamiento de los recursos y herramientas que el propio Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales INAI ha dispuesto para su uso y obtención de beneficios, se propone se desarrolle un programa que considere los siguientes elementos, y que dentro de su alcance se integre a todos los servidores públicos que intervienen en el tratamiento de datos personales, como sigue:

I) Introducción al derecho a la protección de datos personales.

- ✓ Principios
- ✓ Deberes
- ✓ Sistemas de datos personales
- ✓ Medidas de seguridad
- ✓ Procedimientos y sanciones/ Derechos ARCO (acceso, rectificación, cancelación y oposición)
- ✓ Medios de defensa

II) Introducción sobre la LGPDPPSO y su reglamento.

- ✓ Antecedentes.
- ✓ ¿A quién aplica?
- ✓ ¿Qué objeto tiene?

III) Fundamentos conceptuales de la LGPDPPSO.

- ✓ Encargado, Responsable y Titular.
- ✓ Dato Personal y Dato Personal Sensible.
- ✓ Inventario y Base de Datos.
- ✓ Medidas de seguridad.

IV) Análisis de brecha y de riesgo.

- ✓ Resultado negativo.
- ✓ Resultado positivo.

V) Prevenciones y recomendaciones.

- ✓ Multas, sanciones y auditorías.
- ✓ Principios legales.

8. Funciones y responsabilidades del tratamiento de datos personales.

De conformidad con el artículo 3, fracción XXII y XXIII y de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los servidores públicos de la ASIPONA Manzanillo que recaben, traten y resguarden datos personales en el ejercicio de sus funciones y atribuciones respecto a la Unidad Administrativa a la que se encuentren adscritos, observarán al menos, las medidas de seguridad físicas y técnicas siguientes:

- **Medidas de seguridad físicas:**
  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:**
  a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
  b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
  c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
  d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;

Adicionalmente, los servidores públicos de la ASIPONA Manzanillo, al tratar los datos personales, observarán las siguientes funciones y obligaciones:

Funciones:

- Resguardar los datos personales a los que tengan acceso en el ejercicio de sus atribuciones.
- Verificar que el inventario de datos personales y de los sistemas de tratamiento de los mismos, a los que tienen acceso, se encuentren actualizados.
- 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.

- Mantener actualizada la relación de usuarios que traten datos personales.
- En caso de que se presente algún incidente de vulneración de seguridad de los datos personales y/o de los sistemas de tratamiento de los mismos, informar dicho incidente a la Unidad de Transparencia y llevar el registro de los hechos.

Derivado de lo anterior, el Comité de Transparencia como autoridad máxima en materia de protección de datos personales, supervisará en coordinación con la Subgerencia de Informática y el Área Coordinadora de Archivo, el cumplimiento de las medidas, controles y acciones previstas en el presente documento de seguridad.

9. Vulneraciones a la seguridad de los datos personales.

Las vulneraciones de seguridad pueden detonarse a partir de una amenaza y/o debilidad en el sistema de tratamiento de datos personales, las cuales, de no ser solventadas de forma inmediata y correcta, son proclives a convertirse en un riesgo materializado; es decir, en una afectación concreta al sistema que contiene datos personales.

Por tal motivo, el presente documento tiene como propósito establecer los parámetros que serán considerados ante una eventual vulneración de datos.

1. Las vulneraciones de seguridad se caracterizan por:

a) Afectar los sistemas relacionados con los datos personales en cualquier fase de su tratamiento, y

b) Afectar de manera significativa los derechos patrimoniales o morales de los titulares de los datos personales.

2. Se considerarán como vulneraciones de seguridad, las siguientes:

a) La pérdida o destrucción no autorizada;

b) El robo, extravío o copia no autorizada;

c) El uso, acceso o tratamiento no autorizado; o

d) El daño, la alteración o modificación no autorizada.

3. En caso de que se materialice una vulneración, y en el supuesto de que la Subgerencia de Informática y/o el área Coordinadora de archivo sean quienes en primera instancia tengan conocimiento de la afectación, éstas deberán comunicarlo el mismo día hábil de su conocimiento, a la o a las unidades responsables del sistema de tratamiento de datos personales.

4. En cuyo caso de que la Subgerencia de Informática y/o el área Coordinadora de archivo no remitan el informe de la vulneración a la unidad responsable, en el periodo de tiempo estimado por el presente manual, se dará vista a su superior jerárquico, el cual deberá remitir un informe que justifique la falta de alertamiento a la unidad responsable.

5. En caso de que el superior jerárquico no remita el reporte sobre la vulneración a un sistema de datos personales, se procederá a dar vista al Órgano Interno de Control para el inicio de un procedimiento disciplinario administrativo.

6. Si la unidad responsable es la primera instancia que tiene conocimiento de la vulneración, ésta deberá consultar a la Subgerencia de Informática y/o el área.

7. Coordinadora de archivo la gravedad de la afectación, cuando corresponda a medidas de seguridad implementadas por dichas unidades. La consulta en comento deberá realizarse a más tardar el día hábil siguiente a la identificación de la vulneración, y la respuesta a la misma, deberá otorgarse a más tardar el día hábil siguiente a su recepción.

8. En caso de que la unidad responsable no remita la consulta a la Subgerencia de Informática y/o el área Coordinadora de archivo, en el periodo de tiempo estimado por el presente manual, se dará vista a su superior jerárquico, el cual deberá remitir un informe que justifique la falta de conocimiento a la unidad responsable.

9. En caso de que el superior jerárquico no remite el reporte sobre la vulneración a un sistema de datos personales, se procederá a dar vista al Órgano Interno de Control para el inicio de un procedimiento disciplinario administrativo.

10. En el supuesto de que Subgerencia de Informática y/o el área Coordinadora de archivo no remitan en tiempo y forma la consulta pedida por la unidad responsable se dará vista a su superior jerárquico el cual deberá remitir un informe que justifique la falta de alertamiento a la unidad responsable.

11. En el supuesto de que el titular sea quien identifique que sus datos personales han sido comprometidos, y lo informe a través de una queja, la Unidad de Transparencia deberá comunicarlo a la o a las unidades responsables del sistema de tratamiento de datos personales afectados, el mismo día hábil de su conocimiento.

12. Una vez que se haya confirmado la vulneración, la unidad responsable deberá notificar al titular de los datos, así como al INAI, en un plazo no mayor a las 72 horas siguientes.

13. La notificación al titular se realizará preferentemente de forma directa, ya sea por teléfono, correo electrónico, correo postal, o en persona. En caso de que exista urgencia para contactar al titular, se podrá utilizar más de un medio de contacto a la vez.

14. Se puede optar por la notificación indirecta a través de sitios web o medios de comunicación masivos, solamente cuando la notificación directa pueda causar más afectaciones al titular, sea muy costosa o no se tenga información de contacto.

15. La notificación al titular deberá contener lo siguiente:

a) Descripción de la vulneración: Se debe explicar de manera muy sencilla y general el incidente ocurrido, en qué consistió, el periodo en el

que se desarrolló. No se deben dar detalles o incluir información que revele vulnerabilidades o fallas específicas en los sistemas de tratamiento.

b) Datos personales involucrados: Una descripción de la información involucrada en el incidente.

c) Recomendaciones a los titulares: El listado de acciones que puede realizar el titular para minimizar los efectos adversos de la vulneración.

d) Acciones correctivas o de mitigación: Una descripción general de las acciones llevadas a cabo para evitar que incidentes similares se repitan.

e) Los medios donde los titulares pueden obtener más información: Datos de las unidades designadas, mesas de servicio o del personal del responsable que puede atender dudas y proporcionar información adicional del incidente.

f) La descripción de las circunstancias generales en torno a la vulneración ocurrida, que ayuden al titular a entender el impacto del incidente.

g) Fuentes de información adicional: Referencias o documentos adicionales de consulta para apoyar a los titulares ante situaciones específicas, como el robo de identidad, en su caso.

16. La notificación de vulneración al INAI se realizará por la unidad responsable y podrá ejecutarse mediante escrito presentado en el domicilio del Instituto, o bien, a través de cualquier otro medio que se habilite para tal efecto.

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

a) La hora y fecha de la identificación de la vulneración;

b) La hora y fecha del inicio de la investigación sobre la vulneración;

c) La naturaleza del incidente o vulneración ocurrida;

d) La descripción detallada de las circunstancias en torno a la vulneración ocurrida;

e) Las categorías y número aproximado de titulares afectados;

f) Los sistemas de tratamiento y datos personales comprometidos;

g) Las acciones correctivas realizadas de forma inmediata;

h La descripción de las posibles consecuencias de la vulneración de seguridad ocurrida;

i) Las recomendaciones dirigidas al titular;

j) El medio puesto a disposición del titular para que pueda obtener mayor información al respecto;

k) El nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar mayor información al Instituto, en caso de requerirse, y

l) Cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

18. La unidad 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 que se elabore una bitácora de las vulneraciones, en la que se describen éstas, la fecha en la que ocurrieron, el motivo y las acciones correctivas implementadas.

19. Posteriormente a la confirmación y notificación de la vulneración de seguridad, la unidad responsable deberá realizar las acciones correctivas necesarias en coordinación con la Subgerencia de Informática y el área Coordinadora de archivo, para mitigar el riesgo en cualquier sistema de seguridad de datos personales.

20. Las unidades responsables, con la asesoría de la Subgerencia de Informática y el área Coordinadora de archivo y apoyo de la Unidad de Transparencia, deberán continuar con la implementación de medidas de seguridad que permitan mejorar la atención y detección de nuevas vulneraciones, así como la respuesta cuando éstas ocurran.

21. Las acciones que implemente la Subgerencia de Informática y el área Coordinadora de archivo deberán atender las obligaciones que les confiere el Programa de Datos Personales de la ASIPONA Manzanillo, el cual tiene como objeto implementar un sistema de datos personales que integre las medidas de seguridad correspondientes a todos los sistemas de datos personales, así como un documento de seguridad.

22. Dichos procedimientos serán gratuitos para los titulares, de fácil acceso y con la mayor cobertura posible, debidamente habilitados y disponibles en todo momento.