GOBIERNO DEL ESTADO
2022 | 2027

IQTP
INSTITUTO
QUINTANARROENSE
DE TRANSPARENCIA
PARA EL PUEBLO

DOCUMENTO ORIENTADOR PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE PROTECCIÓN DE DATOS PERSONALES

Índice

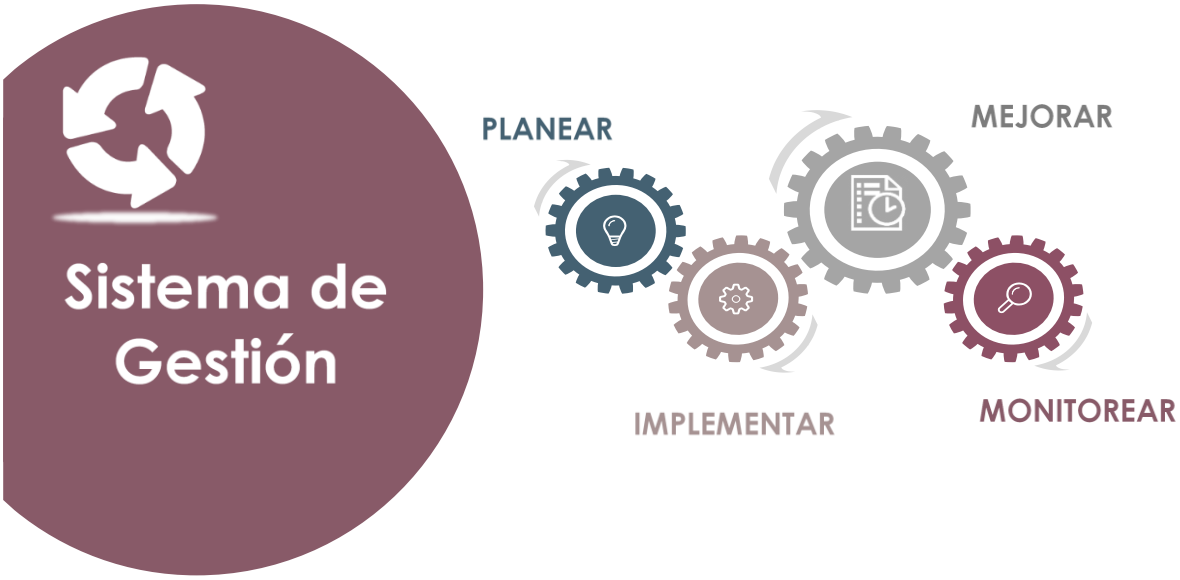
Introducción

El presente documento tiene como objeto ser una guía de apoyo para los Sujetos Obligados en la realización e implementación de su Sistema de Gestión de Seguridad, como parte del acompañamiento del Instituto Quintanarroense de Transparencia para el Pueblo (IQTP), en el cumplimiento a las disposiciones establecidas en el artículo 34, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo (LPDPPSOQROO).

Es menester aclarar que se trata de una guía de acompañamiento para los Sujetos Obligados, y no un formato obligatorio, ya que los responsables del tratamiento de los datos personales pueden utilizar cualquier estilo o formato, siempre y cuando atiendan a cabalidad con las disposiciones de la Ley.

Una de estas obligaciones es documentar las acciones relacionadas con las medidas de seguridad en el tratamiento de los datos personales, en un SGDP. Entendiendo éste, como el conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

Ahora bien, para el desarrollo de este Sistema de Gestión para la Protección



de los Datos Personales, el Instituto propone implementar el siguiente programa integrado por cuatro fases planeación y diagnóstico, desarrollo, implementación y control.

GLOSARIO

Activo. La información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado con el tratamiento de datos personales, que tenga valor para el Sujeto Obligado.

Administrador. La persona servidora pública o persona física facultada y nombrada por el responsable para llevar a cabo tratamiento de datos personales y que tiene bajo su responsabilidad los sistemas y bases de datos personales.

Amenaza. Circunstancia o evento con la capacidad de causar daño a un sujeto obligado

Análisis de brecha. Análisis entre las medidas de seguridad existentes y aquellas que resulten necesarias para la seguridad de los datos personales.

Análisis de riesgos. Estudio de las causas de posibles amenazas y probables eventos no deseados de los daños y consecuencias que estas puedan producir.

Áreas o Unidades Administrativas. Las instancias que pertenecen a los sujetos obligados que cuenten o puedan contar, dar tratamiento y ser responsables o encargados, personas usuarias de los sistemas y bases de datos personales previstos en las disposiciones legales aplicables.

Bases de Datos. El conjunto ordenado de datos personales referentes a una persona física identificada o identificable.

Bloqueo. La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas.

Diagnóstico. Análisis que se realiza para determinar cualquier situación y cuáles son las tendencias.

Durante dicho período, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda.

Fuentes de acceso público. Aquellas bases de datos, sistemas o archivos que por disposición de la ley puedan ser consultadas públicamente, cuando no exista impedimento por una norma limitativa y sin más exigencia en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita.

Impacto. Una medida del grado de daño a los activos o cambio adverso en el nivel de los objetivos alcanzados en una organización.

Incidente. Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.

Instituto. Instituto Quintanarroense de Transparencia para el Pueblo (IQTP).

Ley. Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo.

Persona Encargada. A la persona física o moral, 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.

Persona Titular. A la persona a quien corresponden los datos personales.

Responsable. Los Sujetos Obligados a que se refiere la Ley de Datos que deciden sobre el tratamiento de los datos personales.

Remisión. A toda comunicación de datos personales realizada exclusivamente entre el responsable y la persona encargada, dentro o fuera del territorio mexicano.

Riesgo. Combinación de la probabilidad de un evento y su consecuencia desfavorable.

Riesgo de Seguridad. Potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de una organización.

- **Identificar el riesgo.** Proceso para encontrar, enlistar y describir los elementos del riesgo.
- **Valorar el riesgo.** Proceso para asignar valores a la probabilidad y consecuencias del riesgo.
- **Comunicar el riesgo.** Compartir o intercambiar información entre la alta dirección, custodios y demás involucrados acerca del riesgo.
- **Tratar el riesgo:** Procesos que se realizan para modificar el nivel de riesgo.
    - Aceptar el riesgo. Decisión informada para coexistir con un nivel de riesgo.
    - Compartir el riesgo. Proceso donde se involucra a terceros para mitigar la pérdida generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad.

- Evitar el riesgo. Acción para retirarse de una situación de riesgo o decisión para no involucrarse en ella.
- Reducir el riesgo. Acciones tomadas para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas al riesgo.
- Retención del riesgo. Aceptación de la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido.
- Riesgo residual. El riesgo remanente después de tratar el riesgo.

SGDP. Sistema de Gestión para la Protección de los Datos Personales

Sistema de Gestión de Seguridad de Datos Personales (SGSDP). Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley.

Seguridad de la información. Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

- **Confidencialidad.** Propiedad de la información para no estar a disposición o ser revelada a personas, entidades o procesos no autorizados.
- **Disponibilidad.** Propiedad de un activo para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.
- **Integridad.** La propiedad de salvaguardar la exactitud y completitud de los activos.

Transferencia. A toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta de la titular, del responsable o de la persona encargada.

Tratamiento. A 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, y

Vulnerabilidad. Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

Fases	Procesos	Actividades
Fase 1	Planeación y Diagnóstico del SGSD	1.1 Definir el alcance y los objetivos del SGDP.
		1.2 Elaboración del documento descriptivo de las etapas de SGDP.
		1.3 Elaboración de diagnóstico del tratamiento de datos personales.
		1.4 Reunión con los titulares de las Unidades Administrativas del Sujeto Obligado para presentar el calendario.
		1.5 Visita a las áreas administrativas del Sujeto Obligado para la aplicación de diagnóstico.
Fase 2	Desarrollo	2.1 Elaboración de Inventario de Datos Personales con los resultados del diagnóstico.
		2.2 Identificación de funciones y obligaciones de las personas servidoras públicas que realizan tratamiento de datos personales.
		2.3 Realización del análisis de riesgos e identificación de medidas de seguridad.
		2.4 Realización del análisis de brecha para la identificación de las condiciones adecuadas a implementar.
		2.5 Creación de políticas internas y medidas preventivas, para la gestión, tratamiento y protección de los datos personales.
Fase 3	Implementación	3.1 Elaboración del Plan de Trabajo para instrumentar las medidas necesarias en el Sistema de Gestión.
		3.2 Implementar el Plan de Trabajo diseñado.
Fase 4	Control	4.1 Establecimiento de procesos de evaluación continua y monitoreo de las medidas implementadas y/o riesgos que se pudieran generar (auditorias y revisiones).
		4.2 Diseño de programas de capacitación para el personal que interviene en el tratamiento de los datos personales.

Cabe mencionar que cada Sujeto Obligado deberá implementar su propio Sistema de Gestión de acuerdo con sus funciones y necesidades, deberán revisar analíticamente si requieren alguna actividad adicional o si ya cumplen con algunas de las propuestas.

Las siguientes etapas y fases son ejemplos ilustrativos más no limitativos.

1. Planeación y diagnóstico.

1.1 Definir el alcance y los objetivos.

Alcance.

Se establecerá un alcance para el flujo y tratamiento de los datos personales, así como el ciclo vida de estos, al interior y en su caso, al exterior del Sujeto en su calidad de responsable. Se tomará en cuenta lo siguiente:

- Obtención de los datos personales. (cómo se recaban).
- Uso de los datos personales conforme a las finalidades previstas.
- Áreas Administrativas que dan tratamiento a datos personales.
- Administrador o administradores de sistemas y/o bases de datos Personales.
- Registro de los sistemas y/o bases de datos personales.
- Mecanismos, procedimientos y tecnologías utilizados en el tratamiento de los datos personales.
- Modo y espacio de almacenamiento.
- Período de conservación de los datos personales.
- Supresión y/o borrado seguro de los datos personales al concluir el tratamiento.
- Mecanismos preestablecidos para las transferencias de datos personales.
- Marco regulatorio del responsable.

Objetivos.

Establecer los objetivos generales que puedan ser medibles y cuantificables. Con la finalidad determinar las metas y resultados esperados con la implementación del Sistema de Gestión de Seguridad. En concordancia con lo siguiente:

- Cumplimiento a la Ley.
- Cumplir con los principios rectores de Protección de Datos Personales.
- Identificar los tratamientos y ciclos de vida de los datos personales.
- Registrar los Sistemas y Bases de Datos Personales.
- Adoptar, implementar y documentar las medidas de seguridad de carácter físicas, administrativas y técnicas para los sistemas y/o bases de datos personales.
- Establecer las obligaciones y funciones de las personas servidoras públicas en el tratamiento de los datos personales.

- Identificar transferencia de datos personales.
- Prevenir las violaciones a la seguridad de los Sistemas y/o Bases de Datos Personales.

1.2 Elaboración del documento descriptivo de las etapas del SGDP.

Se deberá elaborar un documento para describir las fases y procesos que componen la elaboración del SGDP, mismo que será compartido con las áreas del Sujeto Obligado que realizan tratamiento de datos personales para facilitar su colaboración en las distintas fases que se delinearán dentro de este documento.

1.3 Elaboración del diagnóstico del tratamiento de los datos personales.

Se diseñará un diagnóstico que permita recabar la información necesaria de las áreas sobre el tratamiento que realizan de los datos personales, las medidas y el tipo de seguridad con que cuentan. Asimismo, les permitirá elaborar el inventario de datos personales y el documento que contenga las funciones y obligaciones del personal que maneja o tiene acceso a los datos personales.

1.4 Reunión con las áreas administrativas para la presentación del calendario.

Se convocará una reunión con las personas titulares de las áreas administrativas para darles a conocer el calendario de trabajo y el documento descriptivo, con la finalidad de que otorguen las facilidades requeridas para el desarrollo de las actividades descritas en el material que se hará de su conocimiento.

1.5 Visita a las áreas administrativas del Sujeto Obligado para la aplicación de diagnóstico.

Se realizarán visitas a las áreas administrativas para la aplicación del diagnóstico y la observancia de las medidas de seguridad existentes esto con la finalidad de detectar vulnerabilidades o riesgos que pudiesen ser considerados en las actividades subsecuentes del SGDP.

2. Desarrollo

Con base a lo que señala el artículo 32 de la Ley, 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:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento de datos personales;

IV. 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 más no limitativa, hardware, software, personal del responsable, entre otros;

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

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;

VII. 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, y

VIII. 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.

2.1 Elaboración de inventario de datos personales con los resultados del diagnóstico.

Con la información recopilada se deberá elaborar un inventario de los sistemas y/o bases de datos; así como de los datos personales que los integran. Asimismo, contar con un adecuado inventario de las bases y/o Sistemas de Datos Personales, nos permitirá identificar y vincular la Información, permitiendo conocer el tipo de tratamiento al que serán

sometidos los datos personales relacionándose de manera directa con el flujo y su ciclo de vida.

Con relación a lo anterior, cada Sujeto Obligado determinará, a través de su **titular, órgano competente o Comité de Transparencia**, la creación, modificación o supresión de sistemas y/o bases de datos personales, conforme a su respectivo ámbito de competencia.

A través de la creación de dicho sistema o base de datos personales, el responsable en el tratamiento de la información deberá indicar diversas cuestiones, como lo son:

- El tipo de datos personales objeto del tratamiento.
- La normatividad aplicable en su tratamiento.
- La finalidad del tratamiento.
- El origen, la forma de recolección y actualización de los datos personales.
- El modo de interrelacionar la información.
- El tiempo de conservación de los datos personales.
- Nivel de seguridad que deberá tener de acuerdo con el tipo de tratamiento y con lo anterior definir la medida de seguridad.

Al llegar a esta etapa ya se tiene identificado el ciclo de vida de los datos personales bajo la custodia del Sujeto Obligado y principalmente saben si están controlando la armonía de dicho ciclo: **obtención, uso, comunicación de datos a terceros, si se respaldan, su bloqueo y finalmente la destrucción segura.**

2.2 Identificación de funciones y obligaciones de las personas servidoras públicas que realizan tratamiento de datos personales.

Una vez que se tiene plenamente identificado los datos que se tratan en cada área, así como las medidas de seguridad, se deberán documentar las actividades del personal que interviene en el tratamiento de la información.

Así, el **Principio de Licitud** refiere que el tratamiento de los datos personales deberá de sujetarse a las facultades y atribuciones que los ordenamientos legales les confieran.

Lo anterior en estrecha relación al **Principio de Finalidad**, el cual establece que todo tratamiento de datos personales deberá de estar justificado por finalidades concretas, lícitas, explícitas y legítimas, las cuales deberán de estar relacionadas con las atribuciones que la normatividad aplicable le

confiera, es decir, todo tratamiento de datos personales que realicen los Sujetos obligados debe de contar con el fundamento legal que le permitan llevarlo a cabo.

Aunado a lo anterior, se deberá dar a conocer entre las personas involucradas en el tratamiento de la información las siguientes actividades:

a) Comunicar a todas las personas involucradas en el tratamiento de datos personales la importancia de cumplir y mantener las medidas de seguridad, conociendo los objetivos de su implementación, así como lo relativo a su mejora continua.

b) Establecer los roles, responsabilidades, definir la estructura organizacional del Sujeto Obligado para poder señalar concretamente facultades y atribuciones de las áreas o unidades administrativas que intervengan en el tratamiento de datos personales.

c) Verificar que el personal de las áreas o unidades administrativas conozcan sus atribuciones y la forma de llevarlas a cabo.

Se deberán de adoptar por parte del Sujeto Obligado las medidas necesarias para que el personal que interviene en el tratamiento de los datos personales conozca las normas que son aplicables en el desarrollo de sus actividades, así como las responsabilidades y consecuencias en que pudiera incurrir en caso de incumplimiento.

El Sujeto Obligado deberá de adoptar las medidas pertinentes para que los involucrados en el tratamiento de datos personales tengan acceso autorizado únicamente a aquella información que precisen para el desarrollo de sus funciones.

2.3 Realización de análisis de riesgos e identificación de medidas de seguridad.

Una vez analizada la información respecto del tratamiento de datos personales que lleva a cabo el responsable, así como las funciones y obligaciones de las personas servidoras públicas que intervienen; determinando el tipo, naturaleza y características, se deberá llevar a cabo el análisis de los riesgos a los que pueden ser objeto los datos personales que se encuentren en posesión del Sujeto Obligado.

El análisis de riesgos deberá tomar en consideración lo establecido en el artículo 31 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo, que se detalla a continuación:

I. El riesgo inherente de los datos personales tratados;

II. La sensibilidad de los datos personales tratados;

III. El desarrollo tecnológico;

IV. Las posibles consecuencias de una vulnerabilidad para las personas titulares;

V. Las transferencias de datos personales que se realicen;

VI. El número de personas titulares;

VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y

VIII. 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.

El análisis tendrá como objetivo el establecimiento de los riesgos a los que está sujeta la información en tratamiento, tomando en consideración las amenazas y vulneraciones identificadas; para adoptar e implementar los controles y medidas de seguridad, con las cuales, se buscará su mitigación y/o erradicación.

En pro de las mejores prácticas, la Metodología BAA (Beneficio para el atacante, la Accesibilidad para el atacante y la Anonimidad del atacante) publicada en junio del 2015, por el hoy extinto Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), ha sido integrada en parte para que el responsable pueda entender mejor lo que se refiere al análisis de riesgo, para más información se recomienda que se consulte la citada metodología.

Análisis de Riesgos conforme a la Metodología BAA

El proceso de análisis de riesgos considera la evaluación cuantitativa y cualitativa sobre la posibilidad de que un activo de información pueda sufrir una pérdida o daño. Contempla la identificación de activos, el estudio de causas y consecuencias de las amenazas y vulnerabilidades en los sistemas de tratamiento de datos personales, y permite establecer parámetros para ponderar los efectos de posibles vulneraciones de seguridad. Esta metodología en particular contempla tres factores que en conjunto determinan el riesgo latente de los datos personales (Figura 1):

• **Beneficio**: Factor que deriva en el nivel de riesgo por tipo de dato, determinado por el riesgo inherente del dato y el volumen de titulares de las que se tratan datos.

• **Accesibilidad**: Factor que determina el nivel de riesgo por tipo de acceso, es decir, el número de accesos potenciales a los datos.

• **Anonimidad**: Factor que determina el nivel de riesgo por tipo de entorno desde el que se tiene acceso a los datos. Estos factores de riesgo nos permiten obtener un valor cuantitativo del nivel de riesgo latente de cada particular con relación al tratamiento de datos personales y sensibles y, a partir de ello, una lista de controles congruentes para disminuir los posibles impactos a los datos personales o sensibles.

En la siguiente imagen se ilustra el procedimiento de obtención del valor de riesgo latente:

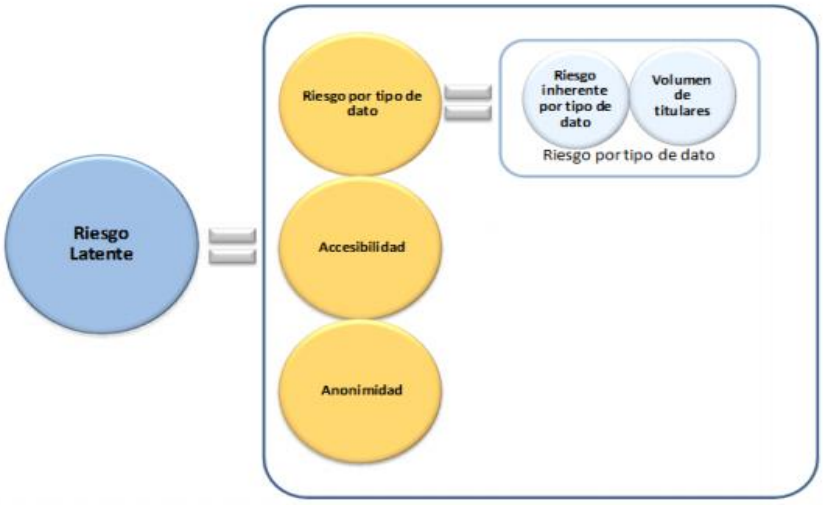


Figura 1. Cálculo de riesgo latente

El nivel de riesgo por tipo de dato es igual al beneficio que representa la información para un atacante, y para calcularlo se requieren dos elementos principalmente:

1. Tener el nivel de riesgo inherente de cada tipo de dato que se trate, y;

2. Calcular el volumen de personas titulares, cuantificando el número de personas de las que se traten datos personales.

Figura 2. Identificación de riesgo por tipo de dato

El nivel de riesgo inherente de cada tipo de dato se determina de acuerdo con la sección 2. Identificación y clasificación de datos personales. Mientras que el volumen de personas titulares se calcula acotando la cantidad de personas en un sistema de tratamiento de datos personales:

<500: Datos hasta 500 personas.
<5k: Datos entre 501 hasta 5,000 personas.
<50k: Datos entre 5,001hasta 50, 000 personas.
<500k: Datos entre 50,001 hasta 500, 000 personas.
>500k: Datos de más de 500, 000 personas

Es importante que para llevar a cabo la cuantificación de personas titulares se considere tanto los soportes físicos, como los electrónicos. Se debe seleccionar uno de los rangos anteriores según el tipo de dato y su nivel de riesgo inherente, por ejemplo:

Tipo de dato	Nivel de riesgo inherente	Volumen de las personas titulares
Patrimoniales	Medio	50K

Al definir el nivel de riesgo inherente por cada tipo de dato y el volumen de personas titulares, se podrá identificar el nivel de riesgo por tipo de dato que se trata en la organización. Se han establecido cinco niveles posibles (Figura 3) nombrados con valor numérico del 1 al 5, tal como se muestra en la siguiente imagen, donde 1 es el nivel más bajo y 5 el más alto:

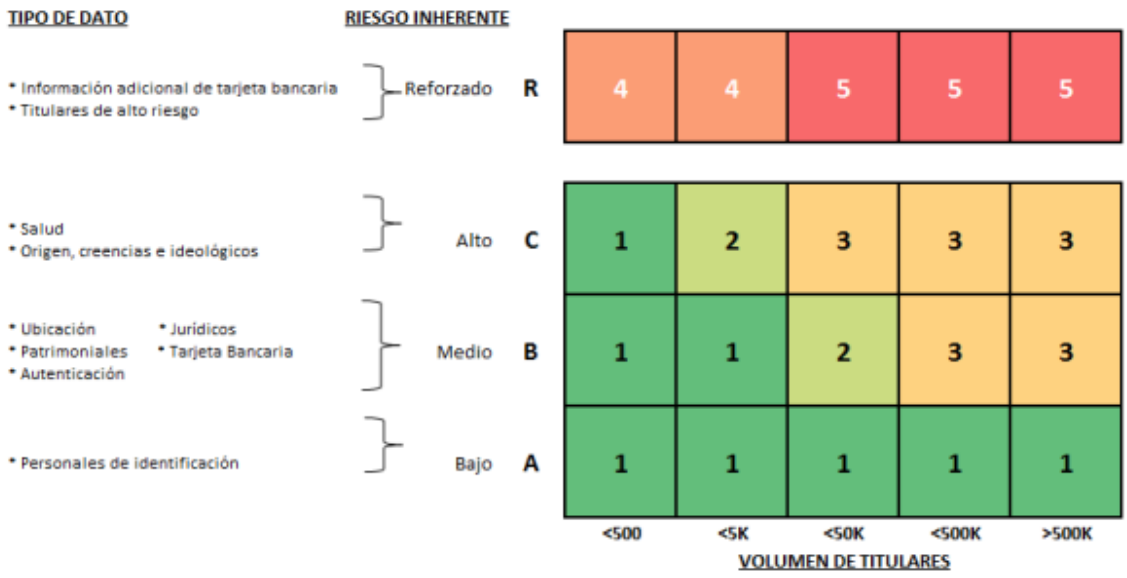


Figura 3. Nivel de riesgo por tipo de dato

A continuación, se detallan los niveles mencionados:

Riesgo por tipo de dato Nivel 1, ocurre cuando:

- El nivel de riesgo inherente de los datos sea bajo, sin importar el número de personas
- El nivel de riesgo inherente sea medio y se tengan hasta cinco mil (5,000) personas
- El nivel de riesgo inherente sea alto y se tengan hasta quinientas (500) personas

Riesgo por tipo de dato Nivel 2, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea medio y se tengan hasta cincuenta mil (50,000) personas
- El nivel de riesgo inherente de los datos personales sea alto y se tengan hasta cinco mil (5,000) personas

Riesgo por tipo de dato Nivel 3, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea medio y se tenga de cincuenta mil (50,000) personas en adelante
- El nivel de riesgo inherente de los datos personales sea alto y se tenga de cinco mil (5,000) personas en adelante

Riesgo por tipo de dato Nivel 4, ocurre cuando:

- El nivel de riesgo inherente de los datos personales sea reforzado y se tengan hasta cinco mil (5000) personas.

Riesgo por tipo de dato Nivel 5, ocurre cuando:

• El nivel de riesgo inherente de los datos personales sea reforzado y se tengan más de cinco mil (5,000) personas.

En la Tabla 2 se muestra una relación del tipo de datos con el nivel de riesgo correspondiente.

Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares				
		<500k	<5k	<50k	<500k	>500k
Ubicación en conjunto con patrimoniales	REFORZADO	4	4	5	5	5
Información adicional de tarjeta bancaria	REFORZADO	4	4	5	5	5
Titulares de alto riesgo	REFORZADO	4	4	5	5	5
Salud	ALTO	1	2	3	3	3
Origen, creencias e ideológicos	ALTO	1	2	3	3	3
Ubicación	MEDIO	1	1	2	3	3
Patrimoniales	MEDIO	1	1	2	3	3
Autenticación	MEDIO	1	1	2	3	3
Jurídicos	MEDIO	1	1	2	3	3
Tarjeta Bancaria	MEDIO	1	1	2	3	3
Personales de identificación	BAJO	1	1	1	1	1

Tabla 2. Nivel de riesgo por tipo de dato

Este nivel de riesgo servirá para determinar los controles que debe considerar el responsable para la protección de datos personales, que se describen respecto a la identificación de medidas de seguridad.

Para efectos de lo anterior, se puede considerar como amenaza aquella que tiene el potencial de dañar la información sometida a tratamiento y causar una vulneración a la seguridad. Se puede considerar que las amenazas son de origen natural o humano, por tanto, pueden ser accidentales o deliberadas; además de provenir de dentro o fuera del responsable.

Por lo que se deberán considerar las amenazas y vulnerabilidades existentes, así como los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, interfaces, documentos electrónicos, entre otros.

Las medidas de seguridad se definen como el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales.

Para llevar a cabo el análisis de riesgo, se deberá de tornar en consideración los siguientes aspectos:

Valoración del riesgo

En esta etapa se identifican los datos personales que deberán de ser protegidos, así como las posibles amenazas y los escenarios de vulneración. Asimismo, determina las consecuencias potenciales de que se presente una vulneración a los datos personales dentro del responsable.

Identificación de amenazas

Una amenaza tiene el potencial de dañar la información y causar una vulneración a la seguridad. Las amenazas pueden ser de origen natural o humano, y pueden ser accidentales o deliberadas y además provenir del interior o del exterior del responsable.

Identificación de vulnerabilidades

Las vulnerabilidades son las debilidades en las medidas de seguridad de los datos personales, pudiéndose identificar en los siguientes ámbitos:

- Organizacionales.
- De procesos y procedimientos.
- De personal.
- Del entorno físico.
- Respecto de los sistemas tecnológicos.
- Respecto de transferencias.
- De la relación con terceros.

Amenazas Típicas

Origen de la amenaza	Motivación/Causa	Posibles consecuencias
Hacker	• Desafío. • Dinero. • Ego. • Estatus. • Rebelión.	• Código malicioso. • Acceso no autorizado al Sistema. • Intrusión en los sistemas. • Robo de información. • Fraude.
Criminal computacional	• Alteración no autorizada de la información. • Destrucción de la información. • Ganancia económica. • Revelación ilegal de la información.	• Acciones fraudulentas, Robo. • Extorsión y chantaje, acoso, • Intrusión a los sistemas informáticos. • Sobornos de Información. • Suplantación de identidad. • Venta de información personal.

Espías (gobiernos, robo de tecnología, etc.)	• Espionaje económico.
	• Ventaja competitiva.
		• Acceso no autorizado a información clasificada.
		• Explotación económica.
		• Intrusión a la privacidad personal.
		  • Penetración en los Sistemas.
		  • Robo de información.
		  • Ventaja política.

Origen de la amenaza	Motivación/Causa	Posibles consecuencias
Interno (personal con poco entrenamiento, descontento, negligente, deshonesto o personas empleadas despedidas)	•Curiosidad. •Ego. •Errores no intencionales u omisiones (Errores de captura de información, errores de Programación). •Ganancia económica. •Venganza	• Abuso de operación de los sistemas. • Acceso no autorizado a los sistemas. • Ataque a las personas empleadas y/o instalaciones. • Chantaje. • Código malicioso. • Consulta de información clasificada o propietaria. • Datos incorrectos. • Errores en los sistemas. • Fraude y robo. • Intercepción de Comunicaciones. • Intrusiones a sistemas. • Sabotaje de los sistemas. • Sobornos de información. • Venta de información • Personal

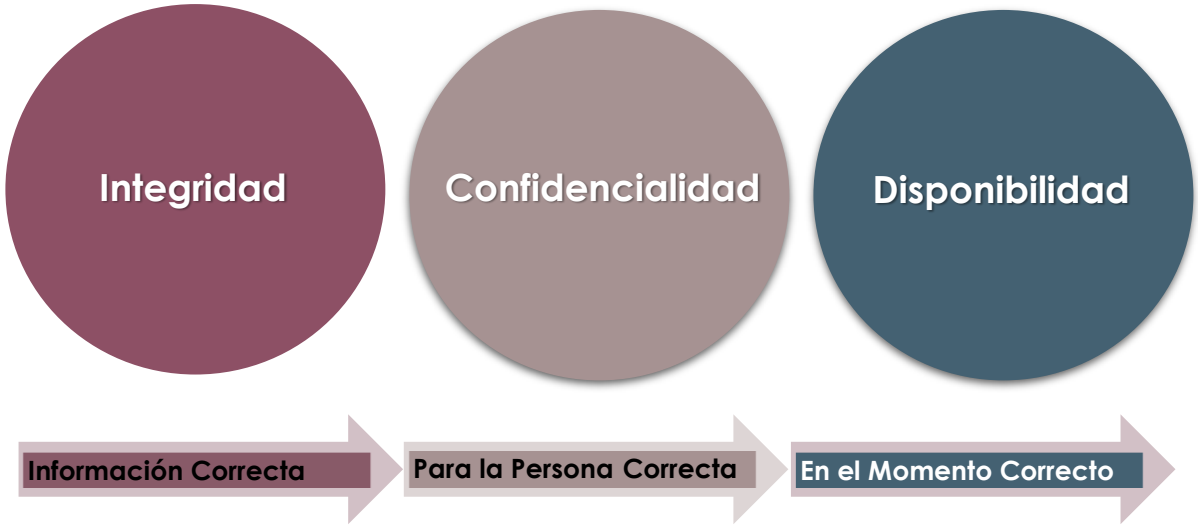
Tipos de amenazas

Tipo	Amenaza
Daño físico	• Fuego. • Agua. • Contaminación. • Accidentes. • Polvo, corrosión, humedad, etc.
Eventos Naturales	• Fenómenos climáticos o meteorológicos. • Fenómenos sísmicos. • Fenómenos volcánicos.
Pérdida de Servicios Básicos	• Falla en el sistema de aire acondicionado o suministro de agua. • Pérdida de suministro eléctrico. • Falla en los equipos de Telecomunicaciones.

Información comprometida por fallas técnicas.	• Intercepción e interferencia de señales. • Espionaje remoto. • Escucha en comunicaciones. • Robo de medios o documentos. • Robo de equipo. • Recuperación de medios desechados o reciclados. • Revelación fuentes poco confiables para la obtención de datos. • Alteración de hardware. • Alteración de software. • Rastreo de localización fallas del equipo. • Malfuncionamiento del equipo. • Saturación de los sistemas de información. • Malfuncionamiento del software. • Falla en el mantenimiento del sistema de información.

Identificar las Medidas de Seguridad

Las medidas de seguridad se definen como el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permiten proteger los datos personales tal y como lo establece la fracción XXII del artículo 3 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo.



Ahora bien, el artículo 30 de la Ley refiere que con independencia del tipo de sistema en el que se encuentran los datos personales o el tipo de tratamiento que se efectúe, el Responsable, deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico, para la protección de los datos personales contra daño, pérdida, alteración, destrucción, o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Las fracciones **XXIII, XXIV** y **XXV** del artículo 3 de la Ley, determina lo que se entenderá por medidas de seguridad administrativas, físicas y técnicas, quedando de la manera siguiente:

Medidas de Seguridad Administrativas: A las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, entre las que podemos destacar:

a) Identificación de la información.

b) Clasificación de la información.

c) Borrado seguro de la información.

d) Sensibilización y capacitación del personal.

Cabe señalar que las Medidas de Seguridad Administrativas, deben implementarse para la consecución de los objetivos contemplados en los siguientes apartados:

•**Política de seguridad**. Definición de directrices estratégicas en materia de seguridad de activos, alineadas a las atribuciones de las dependencias o entidades. Incluye la elaboración y emisión interna de políticas, entre otros documentos regulatorios del Sujeto Obligado.

•**Cumplimiento de la normatividad.** Los controles establecidos para evitar violaciones de la normatividad vigente, obligaciones contractuales o la política de seguridad interna. Abarca, entre otros, la identificación y el cumplimiento de requerimientos tales como la legislación aplicable.

•**Organización de la seguridad de la información.** Establecimiento de controles internos y externos a través de los cuales se gestione la seguridad de activos. Considera, entre otros aspectos, la organización interna, que a su vez se refiere al compromiso de la alta dirección y la designación de

responsables, entre otros objetivos; asimismo, considera aspectos externos como la identificación de riesgos relacionados con terceros.

•**Clasificación y control de activos**. Establecimiento de controles en materia de identificación, inventario, clasificación y valuación de activos conforme a la normatividad aplicable.

•**Seguridad relacionada a los recursos humanos.** Controles orientados a que el personal conozca el alcance de sus responsabilidades respecto a la seguridad de activos, antes, durante y al finalizar la relación laboral.

•**Administración de incidentes.** Implementación de controles enfocados a la gestión de incidentes presentes y futuros que puedan afectar la integridad, confidencialidad y disponibilidad de la información. Incluye temas como el reporte de eventos y debilidades de seguridad de la información.

•**Continuidad de las operaciones.** Establecimiento de medidas con el fin de contrarrestar las interrupciones graves de la operación y fallas mayores en los sistemas de información. Incluye planeación, implementación, prueba y mejora del plan de continuidad de la operación del sujeto obligado.

Medidas de Seguridad Físicas: Al conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades.

a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y

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

Medidas de Seguridad Técnicas: Al conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las

siguientes actividades:

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

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

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

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de los datos personales.

Las Medidas de Seguridad Técnica, son las aplicables a sistemas de datos personales en soportes electrónicos, servicios e infraestructura de telecomunicaciones y tecnologías de la información, entre otras, se prevén las siguientes acciones:

•**Gestión de comunicaciones y operaciones**. Establecimiento de controles orientados a definir la operación correcta y segura de los medios de procesamiento de información, tanto para la gestión interna como la que se lleva a cabo con terceros. Incluye, entre otros aspectos, protección contra código malicioso y móvil, copias de seguridad, gestión de la seguridad de redes y manejo de medios de almacenamiento.

•**Control de acceso**. Establecimiento de medidas para controlar el acceso a la información, activos e instalaciones por parte de los responsables autorizados para tal fin, considerando en ello, la protección contra la divulgación no autorizada de información. Abarca, entre otros temas, gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información.

•**Adquisición, desarrollo, uso y mantenimiento de sistemas de información**. Integración de controles de seguridad a los sistemas de información, desde su adquisición o desarrollo, durante su uso y mantenimiento, hasta su cancelación o baja definitiva. Considera procesamiento adecuado en las aplicaciones, controles criptográficos y seguridad de los archivos de sistema, entre otros.

•**Tipo de soportes: físicos y electrónicos**. Es importante explicar la diferencia entre un soporte físico y un soporte electrónico, debido a que las medidas de seguridad que el Sujeto Obligado implemente para cada sistema de datos

personales están estrechamente relacionadas con el tipo de soportes utilizados. Para lograr lo anterior, es preciso referirse a las definiciones que se prevén en las Recomendaciones emitidas por el hoy extinto INAI:

- **Soportes físicos.** Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados "a mano" o "a máquina", fotografías, placas radiológicas, carpetas, expedientes, entre otros.

- **Soportes electrónicos**. Son los 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, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil. Es preciso señalar que el Sujeto Obligado deberá identificar el tipo de soporte en el que residen los datos personales de cada uno de los sistemas que posee con el propósito de corroborar que las medidas de seguridad implementadas sean aplicables a cada caso. Por tanto, en el Documento de seguridad deberá constar si los datos personales del sistema residen en:

I. Soporte físico;

II. Soporte electrónico; o

III. Ambos tipos de soportes.

Por lo anterior, el Sujeto Obligado, deberá adoptar las medidas de seguridad necesarias conforme a lo siguiente:

Tipos de seguridad:

a. Física. Medida de Seguridad orientada a la protección de instalaciones, equipos, soportes, sistemas o bases de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor.

b. Lógica. Medidas de seguridad de carácter administrativas y de protección que permiten la identificación y autenticación de Usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función.

c. **De desarrollo y aplicaciones.** Las autorizaciones con las que contará la creación o tratamiento de los sistemas o bases de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de las personas usuarias, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así corno las consideraciones especiales respecto de aplicaciones y pruebas. (Medidas de seguridad administrativas y técnicas)

d. **De cifrado.** La implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la seguridad de la información. (Medidas de seguridad técnicas).

e. **De comunicaciones y redes.** Las medidas de seguridad técnicas, así como restricciones preventivas y de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones. (Medidas de seguridad técnicas).

Niveles de seguridad:

Básico. Medidas generales de seguridad cuya aplicación es obligatoria para todos los sistemas y bases de datos personales. Corresponden los siguientes aspectos con los que deberá contar el Sujeto Obligado:

A. Documento de seguridad.
B. Funciones y obligaciones del personal que intervenga en el tratamiento de las bases o sistemas de datos personales.
C. Registro de incidencias.
D. Identificación y autenticación.
E. Control de acceso.
F. Gestión de soportes.
G. Copias de respaldo y recuperación.

Medio. Medidas de seguridad cuya aplicación corresponde a bases o sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo. De manera adicional a las medidas calificadas como básicas, considera los aspectos siguientes:

a) Responsable de seguridad.
b) Auditoría.
c) Control de acceso físico.
d) Pruebas con datos reales.

Alto. Medidas de seguridad aplicables a bases o sistemas de datos concernientes a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad pública, prevención, investigación y persecución de delitos. Además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:

a) Distribución de soportes.
b) Registro de acceso.
c) Telecomunicaciones.

En el nivel de seguridad básico inciso a), se establece el documento de seguridad como una obligación, mismo que describe el artículo 35 de la Ley.

Considerando todo lo anterior, se dictaminarán los resultados del análisis de riesgos, información que permitirá continuar con el siguiente proceso de la segunda fase.

2.4. Realización de análisis de brecha para las condiciones adecuadas a implementar.

Se realizará un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en el Sujeto Obligado.

Como se ha establecido, las medidas de seguridad permiten proteger los datos personales, teniendo el carácter de administrativas, físicas y técnicas, con el análisis de riesgos elaborado, se deberán identificar las medidas de seguridad a implementar mismas que permitan disminuir los riesgos a la protección de los datos personales.

Una vez que se han identificado los datos personales a proteger, así como las amenazas, vulneraciones y los supuestos que pudiesen afectar la protección de la información, se estará en posibilidades de elaborar un análisis de brecha respecto de las medidas de seguridad, en este sentido, para determinar el análisis de brecha se deberá de identificar lo siguiente:

- Las medidas de seguridad implementadas por el Responsable en el tratamiento de los datos personales identificando plenamente aquellas que se encuentran operando correctamente.

- Las medidas de seguridad faltantes por implementar por el Responsable en el tratamiento de los datos personales.

- Las nuevas medidas de seguridad que de implementarse remplazarían a las que actualmente se encuentran funcionado en la organización del responsable del tratamiento. Es importante contar con la identificación de aquellas medidas de seguridad que actualmente se encuentran establecidas y funcionando en el Sujeto Obligado de manera efectiva, así como aquellas medidas faltantes que deban ser implementadas, para que a través de un plan de trabajo se establezca el procedimiento para su ejecución.

No obstante, no se debe dejar de lado que al momento de crear un sistema y/o base de datos personales, se deberá de tomar en consideración las medidas de seguridad que en el diseño del sistema se hayan determinado.

2.5 Creación de las políticas internas y medidas preventivas, para la gestión, tratamiento y protección de los datos personales.

El responsable en el tratamiento de la información de carácter personal tendrá la obligación de desarrollar e implementar políticas internas y medidas preventivas para la gestión, tratamiento y protección de los datos personales, para coadyuvar en la ejecución y cumplimiento de los objetivos establecidos. En este sentido, se tomará en consideración la estructura de los responsables en materia de Protección de Datos Personales, para establecer las acciones que se llevarán a cabo en el SGDP.

Por lo que refiere a la obtención, tratamiento y resguardo de los datos personales, se deberá de cumplir con lo que establecen los principios en materia de protección de datos personales. Al respecto, el Artículo 11 de la Ley de la materia fundamenta dicha obligación, señalando que todo tratamiento de datos personales por parte de los sujetos obligados debe garantizar el cumplimiento irrestricto de estos principios rectores.

Las políticas y medidas preventivas se enfocarán a todos los tratamientos de los datos personales que se encuentran en los sistemas y/o base de datos, así como su ciclo de vida y sus finalidades aceptadas por las personas titulares de la información. La finalidad de estos instrumentos será la de comprometer a los que intervienen en el tratamiento de los datos personales, a observar, vigilar y cumplir con la Ley Local de

Datos Personales, así como la normatividad que resulte aplicable a la materia de protección de datos personales.

Las políticas y medidas preventivas se documentarán para hacerse de conocimiento de las personas involucrados en el tratamiento de los datos personales, tomando en consideración las reglas siguientes:

I. Dar cumplimiento a los principios y deberes en materia de protección de datos personales, que contempla el título segundo de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo, que son: licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información, transparencia y responsabilidad en el tratamiento de datos personales.

II. **Principio de Licitud.** Implica que todo tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.

III. **Principio de Finalidad.** Implica que todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

IV. **Principio de Lealtad.** Implica que el responsable no deberá obtener y tratar datos personales a través de medios engañosos o fraudulentos, y deberá privilegiar la protección de los intereses de la persona titular y la expectativa razonable de privacidad.

V. **Principio de Consentimiento.** Implica que cuando no se actualicen algunas causales de excepción previstas en el artículo19 de la Ley, el responsable deberá contar con el consentimiento previo de la persona titular para el tratamiento de los datos personales. El consentimiento del titular deberá otorgarse de manera: libre, específica e informada.

VI. **Principio de Calidad.** Implica que el responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos se presume que se cumpla con la calidad de los datos personales cuando éstos son proporcionados directamente por la persona titular y hasta que este no manifieste acredite lo contrario y cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten

aplicables, deberán ser suprimidos , previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos, atendiendo los plazos de conservación señalados en el artículo 20 de la Ley .

VII. **Principio de Proporcionalidad.** Implica que el responsable solo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad concreta, explícita, lícita y legítima que justifica su tratamiento. Asimismo, procurará realizar esfuerzos razonables para tratar los datos personales al mínimo necesario, con relación a las finalidades que motivan su tratamiento.

VIII. **Principio de Información.** Implica que el responsable deberá informar a la persona titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

El Aviso de Privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el responsable, asimismo, deberá ponerse a disposición en su modalidad simplificada.

IX. **Principio de Responsabilidad.** Implica que el responsable deberá implementar los mecanismos previstos en el artículo 29 de la Ley para acreditar el cumplimiento de los principios y deberes y obligaciones establecidas en la misma y rendir cuentas sobre el tratamiento de datos personales en su posesión a la persona titular, o a las Autoridades Garantes Estatales, debiendo observar para tal efecto la legislación aplicable en la materia. Así mismo y en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.

X. **Deber de Seguridad.** El responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para 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.

XI. **Deber de Confidencialidad.** El 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 la confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

3. Implementación

3.1 Elaboración del Plan de Trabajo para instrumentar las medidas necesarias en el Sistema de Gestión.

Con la información recabada en las primeras dos fases, se diseñará un Plan de Trabajo con la finalidad de instaurar al interior del Sujeto Obligado las medidas pertinentes que permitan obtener, tratar y resguardar los datos personales de manera segura, de acuerdo con las capacidades del responsable, con base al análisis de brecha realizado y en conjunción con las políticas y medidas preventivas que se aplicarán.

Para la elaboración se deberá considerar lo siguiente:

a) Alcance y objetivos;
b) Resultados del diagnóstico;
c) Informe de las visitas a las áreas del Sujeto Obligado;
d) Inventario de Datos Personales;
e) Inventario de sistemas de datos;
f) Identificación de las Funciones y Obligaciones de las personas servidoras públicas que participan en el tratamiento de Datos Personales.
g) Resultados del Análisis de Riesgos;
h) Resultados del Análisis de Brecha;
i) Las Políticas y Medidas Preventivas Diseñadas;
j) La Selección de Acciones Prioritarias;
k) El periodo en el que se pretenden cumplir estas acciones;
l) Los recursos humanos y materiales necesarios para el cumplimiento;
m) Las acciones que quedan fuera para el plan de trabajo actual y que se consideran en el plan de trabajo siguiente.

3.2 Implementar el Plan de Trabajo.

Se aplicarán las actividades que se definieron en el Plan de Trabajo, estas dependerán de lo identificado por el Sujeto Obligado y la capacidad física y presupuestal para implementarlas.

Se deberá designar un miembro del equipo responsable para la rendición de cuentas de la gestión de los datos personales dentro del sujeto obligado, de modo que tanto el cumplimiento de la Ley de Protección de Datos Personales

en Posesión de Sujetos Obligados del Estado de Quintana Roo, como la política de gestión y seguridad de los datos personales puedan ser demostrados.

El responsable designado deberá estar a cargo del cumplimiento de las políticas en el día a día, esta función debe tener al menos las siguientes responsabilidades:

1. Compromiso total con el cumplimiento de las políticas.
2. Desarrollo y revisión de las políticas.
3. Asegurar la implementación de las políticas.
4. Revisiones de la gestión de las políticas.
5. Revisión de procedimientos donde sean tratados los datos personales.
6. Enlace con las personas a cargo del manejo de riesgos y asuntos de seguridad dentro del Sujeto Obligado.

Cuando el Sujeto Obligado posee múltiples áreas o departamentos que procesan información personal, deberán determinar si es necesario una red de enlaces responsables en protección de datos personales.

4. Control.

4.1 Establecimiento de procedimientos de evaluación continua y monitoreo de las medidas implementadas y/o riesgos que se pudieran generar.

Este punto de la fase 4 consiste en evaluar y medir los resultados de las políticas, procesos, procedimientos y medidas de seguridad, implementados a fin de corroborar que lo instrumentado arroje los resultados esperados, es decir, una mejora perceptible en la protección de los datos personales.

Se debe monitorear y revisar el riesgo con los factores que se generan, con el previo conocimiento de la información que se resguarda, las amenazas inherentes, vulnerabilidades, el impacto y la probabilidad de ocurrencia. Esto nos permitirá identificar en una etapa temprana cualquier cambio en el contexto del alcance y objetivos de las medidas de seguridad y así mantener una visión general de la imagen del riesgo.

Los responsables deben asegurar que los siguientes puntos estén continuamente monitoreados:

- Nueva información que obre en sus áreas o unidades administrativas.
- Modificaciones necesarias a los datos personales como son la migración de sistemas y las transferencias.
- Nuevas amenazas que podrían estar activas dentro y fuera de la organización y que no han sido valoradas.
- La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
- Vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelven a surgir.
- Incidentes y vulneraciones de seguridad.
- Los factores que determinan la probabilidad de ocurrencia y consecuencias podrían cambiar, lo que afectaría el tratamiento.

Los cambios que afecten a los Sujetos Obligados deben ser revisados de manera específica, no obstante que las actividades de monitoreo requieren de regularidad y periodicidad.

Las medidas de seguridad implementadas para la protección de los datos personales deberán ser sometidas a auditoría interna o externa, mediante la cual se verifique el cumplimiento de las disposiciones legales que rigen el tratamiento de datos personales, así como de los procedimientos en materia de seguridad, en caso de realizarse mediante auditoría interna ésta podrá llevarse a cabo por el Órgano de Control Interno del Sujeto Obligado o el Área encargada de la Protección de Datos de ser el caso.

Las revisiones y auditorías, así como diferentes indicadores pueden informar la ocurrencia de vulneraciones a la seguridad de los datos personales en cualquier fase del tratamiento.

La organización debe contar con procedimientos para tomar acciones que permitan el manejo de las vulneraciones de seguridad que puedan ocurrir, considerando al menos:

1. Identificación de la vulneración.
2. Notificación de la vulneración.
3. Solución del incidente.

Lo anterior en observancia al artículo 37, 38, 39, 40 y 41de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo y demás correlativos y aplicables en la materia.

Las revisiones, auditorías y los tratamientos de una vulneración a la seguridad deben estar debidamente documentados, incluyendo un resumen de los hallazgos y los planes para aplicar medidas preventivas y correctivas con objeto de que se cuente con la evidencia suficiente para tomar las acciones necesarias para evitar o mitigar una vulneración a la seguridad de los datos personales.

4.2 Diseño de programas de capacitación.

La mejor medida de seguridad contra posibles vulneraciones es contar con personal consciente de sus deberes respecto a la protección de datos personales, que identifiquen sus atribuciones, facultades o funciones para el adecuado tratamiento de estos. Por ello, se deben establecer y mantener programas de capacitación que mantengan actualizado al personal involucrado en el tratamiento de la información, llevando a cabo al menos las siguientes acciones:

1. Concientización: programas a corto plazo para la difusión en general de la protección de datos personales en el Sujeto Obligado.
2. Capacitación: programas a mediano plazo que tienen por objetivo capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales y;
3. Educación: programa general a largo plazo que tiene por objetivo incluir la seguridad en el tratamiento de los datos personales.

Se debe realizar una detección de necesidades para identificar el nivel y tipo de capacitación necesaria para el personal, de acuerdo con las responsabilidades asignadas y tomando en cuenta su perfil de puesto, especialmente de aquéllos involucrados en el tratamiento de datos personales.

Finalmente se debe evaluar la eficiencia y eficacia de la capacitación, esta evaluación se puede llevar a cabo mediante la aplicación de exámenes teóricos o prácticos que permitan indicar el grado de conocimiento o entendimiento de la capacitación proporcionada o difusión realizada.

Cabe señalar que de conformidad al artículo 91, segundo párrafo de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo, el Comité de Transparencia será la autoridad máxima en materia de Protección de Datos Personales.

De acuerdo con lo anterior y en apego a lo señalado en el artículo 92, fracciones I, II, V, VI y VIII, del citado ordenamiento, el Comité de Transparencia aprobará, supervisará y evaluará las políticas, programas, acciones y demás actividades que correspondan, para el cumplimiento del Sistema de Gestión; el documento de seguridad y el diseño de los programas de capacitación contenidos en dicho Sistema.