DOCUMENTO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES.

INDICE

MARCO NORMATIVO 3

GLOSARIO. 4

INTRODUCCIÓN 8

OBJETIVO DEL DOCUMENTO DE SEGURIDAD. 9

RESPONSABILIDADES. 10

I. POLITICAS INTERNAS. 11

II. INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO. 11

III. LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES 12

IV. ANÁLISIS DE RIESGOS, ANÁLISIS DE BRECHA Y PLAN DE TRABAJO. 12

Análisis de Brecha 16

Plan de Trabajo 16

V. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD. 17

VI. EL PROGRAMA GENERAL DE CAPACITACIÓN. 18

VII. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD. 18

MARCO NORMATIVO

- Artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos Artículo 21 de la Constitución Política del Estado Libre y Soberano de Quintana Roo.
- Ley General de Transparencia y Acceso a la Información Pública.
- Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados.
- Ley General de Archivos.
- Ley de Transparencia y Acceso a la Información para el Estado de Quintana Roo (LTAIPQROO).
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo (LPDPPSOQROO).
- Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la Elaboración de Versiones Públicas. (Lineamientos Generales).
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.
- Lineamientos Generales para Integración, Organización y Funcionamiento de los Comités de Transparencia de los Sujetos Obligados de la Ley de Transparencia y Acceso a la Información Pública para el Estado de Quintana Roo.
- Reglamento de la Administración Pública de Municipio de Tulum, Quintana Roo.

GLOSARIO

Bases de Datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados que permitan su tratamiento, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento u organización.

Ciclo de vida: Tiempo que duración y conclusión del tratamiento de los datos personales, para después ser suprimidos, cancelados o destruidos por parte del responsable.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable expresada en forma numérica, alfabética, alfanumérica, gráfica, fotográfica, acústica o en cualquier otro formato. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas.

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

Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad de carácter técnico, físico y administrativo adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

Finalidad: Los datos personales recabados y tratados tendrán fines determinados, explícitos y legítimos y no podrán ser tratados ulteriormente con fines distintos para los que fueron recabados. Los datos personales con fines de archivo, de interés público, investigación científica e histórica, o estadísticos no se considerarán incompatibles con la finalidad inicial.

Instituto: Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo.

Ley de datos: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan garantizar la confidencialidad, disponibilidad e integridad de los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad a nivel organizacional, identificación, clasificación y borrado seguro de los datos personales, así como la sensibilización y capacitación del personal en materia de protección de datos personales.

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

a) Prevenir el acceso no autorizado al perímetro de la organización del responsable sus instalaciones físicas, áreas críticas, recurso y datos personales.
b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización del responsable, recursos y datos personales.
c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización del responsable.
d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

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

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

Responsable: Cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, Partidos Políticos, Fideicomisos y Fondos Públicos, que decida y determine finalidad, fines, medios, medidas de seguridad y demás cuestiones relacionadas con el tratamiento de datos personales.

Sistema de datos personales: Conjunto de organizado de archivos, registros, ficheros, bases o banco de datos personales en posesión de los sujetos obligados, cualquiera sea la forma o modalidad de su creación, almacenamiento, organización y acceso. Los sistemas de datos personales se distinguen en:

Físicos: Conjunto ordenado de datos de carácter personal que para su tratamiento están contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, estructurado conforme a criterios específicos relativos a personas físicas que permitan acceder sin esfuerzos desproporcionados a sus datos personales.

Automatizados: Conjunto ordenado de datos de carácter personal que permita acceder a la información relativa a una persona física utilizando una herramienta tecnológica.

Soporte electrónico: Son los medios de almacenamiento inteligibles solo 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), tarjetas de memoria (USB y SD) y demás medios de almacenamiento masivo no volátil.

Soporte físico: 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, demás análogos.

Titular: La persona física a quien correspondan los datos personales.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionados de manera enunciativa más no limitativa con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia y en general cualquier uso o disposición de datos personales.

Unidad de Transparencia: Instancia que auxilia, orienta, gestiona, establece, informa, propone, aplica, asesora, registra y realiza las gestiones necesarias para el manejo, mantenimiento, seguridad, y protección de los sistemas de datos personales en posesión del responsable.

Usuario: Persona autorizada por el responsable, y parte de la organización del sujeto obligado, que dé tratamiento y/o tenga acceso a los datos y/o a los sistemas de datos personales.

Vulneración de datos personales: Es la materialización de las amenazas pudiendo estar enfocadas a la pérdida o destrucción no autorizada de los datos personales, el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada.

INTRODUCCIÓN.

La Constitución Política de los Estados Unidos Mexicanos, en su artículo 6, apartado A, fracción II, establece que la información que se refiere a la vida privada de las personas será protegida en los términos y con las excepciones que fijen las leyes. Además, la fracción III, señala que toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de estos.

Por su parte, el artículo 16 Constitucional, señala la prerrogativa que toda persona tiene, a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, y de igual manera, manifestar su oposición al tratamiento, en los términos que fijen las leyes.

Es así como la Ley General de Transparencia y Acceso a la Información Pública en conjunto con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo establece por su parte un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los Sujetos obligados y sus Unidades Administrativas del Municipio de Tulum, Quintana Roo.

De ahí que el presente Documento de Seguridad tiene como propósito establecer el marco de referencia del tratamiento de los datos personales que se llevan a cabo en el Municipio de Tulum, Quintana Roo para mantener vigente y promover la mejora continua en la protección de estos, además de desarrollar buenas prácticas en la materia.

El Municipio de Tulum reconoce el derecho fundamental de protección de datos personales conforme a la Constitución Política de los Estados Unidos Mexicanos, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Estatal de Protección de Datos Personales en Quintana Roo.

OBJETIVO DEL DOCUMENTO DE SEGURIDAD.

Garantizar que todos los tratamientos de datos personales en posesión del H. Ayuntamiento de Tulum cuenten con medidas de seguridad administrativas, técnicas y físicas que aseguren su confidencialidad, integridad y disponibilidad.

De conformidad con elartículo 32 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo, establece que el responsable debe realizar las siguientes actividades interrelacionadas:

- 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;
- Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales
- Elaborar un inventario de datos personales y de los sistemas de tratamiento;
- 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;
- Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;
- 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;
- 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
- 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.

RESPONSABILIDADES.

En apego al artículo 91 párrafo segundo de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo, establece que el responsable en materia de protección de datos personales es el Comité de Transparencia.

Es así como el Sujeto Obligado contará con un Comité, el cual se integrará y funcionará conforme los establece la Ley de Transparencia y Acceso a la Información Pública para el Estado de Quintana Roo y demás normatividad aplicable.

- Dicho órgano, tendrá dentro de sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales. En esa tesitura dicho órgano tiene las funciones siguientes:
- El Comité y la Unidad de Transparencia deberán coordinar, supervisar y verificar todas las acciones relativas a la seguridad de datos personales.
- Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;
- Dar seguimiento y cumplimiento a las resoluciones emitidas por la Secretaría Anticorrupción y Buen Gobierno de la Administración Pública Federal o las Autoridades Garantes Estatales, según corresponda;
- Establecer programas de capacitación y actualización para las personas servidoras públicas en materia de protección de datos personales

I. POLITICAS INTERNAS.

El Sistema de Gestión de Datos Personales es el medio por el cual la Unidad de Transparencia, Acceso a la Información y Protección de Datos Personales del Municipio de Tulum, garantiza el tratamiento de los datos personales que lleva a cabo como parte de sus funciones, desde su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación correspondiente; para lo cual, se establecen políticas y métodos orientados a salvaguardar la confidencialidad, integridad y disponibilidad de estos datos, de acuerdo con Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo.

El Ayuntamiento implementará políticas para el tratamiento de datos desde su obtención hasta su destrucción, garantizando proporcionalidad, licitud, calidad y responsabilidad.

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

Es un control documentado que permite identificar los procesos en los que las unidades administrativas del Instituto tratan datos personales.

Es a través de esas bases de datos en las que se documenta la información básica de cada tratamiento, con independencia de su forma de almacenamiento.

El Municipio de Tulum, se cuenta con 59 áreas administrativas que se tratan datos personales.

Las personas encargadas de llevar a cabo el tratamiento de datos tienen como funciones y obligaciones las siguientes:

- Garantizar la seguridad en el tratamiento de datos personales, esto con la finalidad de evitar algún riesgo, como la pérdida, robo, alteración o acceso no autorizado.

- Garantizar la debida protección de los datos personales, conforme a la Ley de datos y las demás disposiciones aplicables en la materia.
- Imple
- mentar medidas de seguridad físicas, técnicas y administrativas convenientes para el tratamiento diario de los datos personales.
- Garantizar la confidencialidad de los datos personales derivada de los procedimientos que tienen a su cargo.
- Conocer y aplicar las acciones derivadas de este Documento de Seguridad.
- Garantizar el cumplimiento de los derechos ARCO a los titulares de los datos personales.

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

Cada área deberá garantizar confidencialidad, integridad y correcta gestión de los datos personales de conformidad a los artículos 37, 38, 39, 40, 41 y 42 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Quintana Roo, se describen las funciones y Obligaciones del personal involucrado en el tratamiento de datos personales, esto en apego a las facultades establecidas en el Reglamento de la Administración Pública del Municipio de Tulum, Quintana Roo, así como los Reglamentos Internos de las áreas administrativas.

IV. ANÁLISIS DE RIESGOS, ANÁLISIS DE BRECHA Y PLAN DE TRABAJO.

Se aplicará metodología BAA considerando beneficio, accesibilidad y anonimidad del atacante, así como análisis de brecha para mejorar la seguridad institucional.

El análisis de riesgos es un proceso sistemático para conocer y determinar la magnitud de los riesgos a los que se pueden enfrentar el tratamiento de datos personales durante el ciclo de vida. Por lo que este análisis permite determinar cómo es, cuánto vale y cómo está protegido cada activo (identificando posibles problemas), y anticiparse a las futuras dificultades, lo que nos permitirá tomar mejores decisiones y actuar con oportunidad.

De acuerdo con las Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales, emitidas por el INAI, alguno de los incidentes más comunes son los siguientes:

1. Robo de información en documentos y medios de almacenamiento desechados incorrectamente.
2. Empleados que acceden a datos personales sin la autorización correspondiente.
3. Empleados que revelan información a otras personas a través de engaños.
4. Robo o pérdida de equipos de cómputo, laptops, teléfonos inteligentes, tabletas, o memorias extraíbles con información personal.
5. Acceso ilegal a las bases de datos personales por un externo a la organización.

Ahora bien, en el análisis de riesgos deben considerarse los siguientes elementos:

Activos, que se dividen en tres tipos:

- **Activos de información:**
  - Datos personales recabados;
  - Datos generados
- **Activos físicos:**
  - Elementos físicos e infraestructura que soportan los activos de información

- **Activos de Tecnológicos:**
    - Software y redes

La vulneración o de debilidades de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

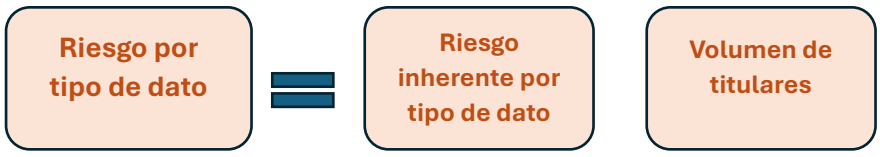
De acuerdo con la **Metodología de Análisis de Riesgo BAA** se enfoca en tres variables que determinan el riesgo latente de los datos personales:

- 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.

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



El volumen de titulares se calcula acotando la cantidad de personas en un sistema de tratamiento de datos personales:

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

TIPO DE DATO PERSONAL	NIVEL DE RIESGO INHERENTE	VOLUMEN DE TITULARES				
		<500	< 5 K	< 50 K	< 500 K	>500k
DATOS DE INDENTIFICACIÓN	BAJO	1	1	1	1	1
ELECTRÓNICOS	BAJO	1	1	1	1	1
ACADÉMICOS	BAJO	1	1	1	1	1
LABORALES	BAJO	1	1	1	1	1
DE RELACIONES PROFESIONALES	BAJO	1	1	1	1	1
FISCALES	MEDIO	1	1	2	3	3
DE RELACIONES COMERCIALES	MEDIO	1	1	2	3	3
SOBRE PROCEDIMIENTOS ADMINISTRATIVOS Y/O JURISDICCIONALES	MEDIO	1	1	2	3	3
PATRIMONIALES	MEDIO	1	1	2	3	3
AFECTIVOS Y/O FAMILIARES	ALTO	2	2	3	3	3
SENSIBLES	ALTO	2	2	3	3	3
DE SALUD	ALTO	2	2	3	3	3
MENORES	ALTO	4	4	5	5	5
UBICACIÓN O DOMICILIO PARTICULAR EN CONJUNTO CON DATOS DE NIVEL MEDIO O ALTO	ALTO	4	4	5	5	5

Análisis de Brecha

Consistente en identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados, cuya información da sustento a las políticas y mecanismos institucionales en materia de protección de datos personales que se deban aprobar. Lo anterior con el objetivo de atenderlas de manera escalonada y en coordinación con cada una de las áreas.

Derivado del análisis fue posible identificar como vulneraciones comunes:

1. Robo de información, modificación-destrucción no autorizada de la información, acceso no autorizado a los sistemas.
2. Daños estructurales, fuego, inundación.
3. Fenómenos climáticos y sísmicos.

Plan de Trabajo

Una vez identificados los factores de riesgo, con los cuales se pueden ver comprometidos los datos personales objetos de tratamiento por parte de las Unidades Administrativas del Municipio de Tulum, Quintana Roo, y con la certeza de identificar a través del análisis de brecha, las medidas de seguridad faltantes o complementarias para cumplir con la correcta protección que conlleve a garantizar la seguridad y confidencialidad, se presentan las acciones a desarrollar, conforme a lo siguiente:

- ✓ Impulsar la capacitación en materia de protección de datos personales a todos las y los servidores públicos de las diversas unidades administrativas.
- ✓ Revisión en la elaboración de avisos de privacidad y establecimiento de medidas de seguridad, así como actualizaciones de estos.
- ✓ Sensibilizar sobre la importancia de la generación de copias de respaldo de la información que contiene datos personales para minimizar el posible daño por pérdida de estos por razones de causas naturales o casos fortuitos.

- ✓ Actualizar el inventario de datos personales para la posible detección de nuevos tratamientos o la modificación de estos.
- ✓ Promover la revisión periódica de las medidas de seguridad.

V. LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD.

Una de las principales acciones del Sujeto Obligado son los mecanismos y revisión de las medidas de seguridad, a fin de detectar posibles inconvenientes y fortalecer dichas medidas.

Dicho lo anterior, se prevé la aplicación de las acciones a realizar por parte de las unidades administrativas que tratan datos personales tales como auditorías periódicas, bitácoras de acceso, mantenimiento preventivo, monitoreo y protocolos para gestión de incidentes, tales como:

- ✓ Mecanismos implementados en el tratamiento de datos personales.
- ✓ Sensibilización y capacitación del personal, en materia de protección de datos personales.
- ✓ Mecanismos para proteger el entorno físico, instalaciones, equipos, soportes o sistemas y datos.
- ✓ Prevención de riesgos por caso fortuito o causas de fuerza mayor.

VI. EL PROGRAMA GENERAL DE CAPACITACIÓN.

Se contempla programa que el Sujeto Obligado deberá capacitarse cuando menos una vez al año, con la intención de que todos los servidores públicos puedan participar y atender temas de Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Principios que regulan el tratamiento de datos personales, deberes y obligaciones de los sujetos responsables, Avisos de Privacidad (integral y simplificado) y Medidas de seguridad orientadas a la protección, seguridad y confidencialidad en el tratamiento de datos personales.

La correcta implementación del Sistema y constante actualización ayuda a mitigar los efectos de una vulneración de datos personales, evita sanciones a servidores públicos responsables en el tratamiento de los datos personales, genera confianza de los titulares hacia el responsable del tratamiento, permite una constante mejora.

VII. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.

Dentro de los mecanismos se cuenta con el propósito de tener una mejora continua, actuar, planificar, verificar y hacer.

Es así como el presente documento de seguridad se actualizará cuando ocurran los siguientes eventos:

- I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, e
- IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.