Documento de Seguridad para la Protección de Datos Personales del Organismo Público Descentralizado Denominado Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública del Estado de Quintana Roo.

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

Creación del Documento de Seguridad para la Protección de Datos Personales del Organismo Público Descentralizado Denominado Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública del Estado de Quintana Roo.

Marco Normativo Aplicable:

- Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Protección de Datos en Posesión de Sujetos Obligados.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo.
- Ley Que Crea el Organismo Público Descentralizado denominado Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública del Estado de Quintana Roo.
- Ley de Transparencia y Acceso a la Información Pública para el Estado de Quintana Roo.
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo
- Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Alcance

Todas las Áreas del Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública del Estado de Quintana Roo.

Anexos:

Anexo 1	Formato de Inventario de Datos Personales y de los Sistemas de Tratamiento
Anexo 2	Inventario de Datos Personales y de los Sistemas de Tratamiento.
Anexo 3	Análisis de Riesgos.
Anexo 4	Análisis de Brecha.
Anexo 5	Plan de Trabajo.
Anexo 6	Mecanismos de monitoreo y revisión de las medidas de seguridad.
Anexo 7	Programa de Capacitación.

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

Considerando

I. Que la Constitución Política de los Estados Unidos Mexicanos, en su artículo 6, Base A, Fracción II refiere que la vida privada y que los Datos Personales serán protegidos con las excepciones que fijen las leyes correspondientes;

II. Que el párrafo segundo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, señala que toda persona tiene derecho a la protección de sus datos personales, al Acceso, Rectificación y Cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

III. Ley General de Protección de Datos en Posesión de Sujetos Obligados, la cual es de aplicación y observancia directa para los sujetos obligados pertenecientes al orden Federal y que en su Transitorio Séptimo establece que los sujetos obligados deberán tramitar, expedir o modificar su normatividad interna a más tardar dentro de los dieciocho meses siguientes a la entrada en vigor del citado Decreto;

IV. Que el Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública es un Organismo Público Descentralizado de la Administración Pública Estatal, cuenta con el carácter de Sujeto Obligado de conformidad con los artículos 1 y 3, Fracción XXVIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;

V. Que en el artículo 34 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo, se señalan las actividades interrelacionadas que deben realizar los responsables para establecer y mantener las medidas de seguridad para la protección de los datos personales. Asimismo, en el artículo 36 de la Ley antes referida se señala la obligación de elaborar un

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

documento de seguridad que cumpla con todos los requisitos establecidos.

VI. Los Lineamientos Generales de Protección de Datos Personales para el Sector Público, mismos que en su artículo 47 cita que el responsable deberá elaborar e implementar políticas y programas de protección de datos personales que tengan por objeto establecer los elementos y actividades de dirección, operación y control de todos los procesos que, en el ejercicio de sus funciones y atribuciones, impliquen un tratamiento de datos personales a efecto de proteger éstos de manera sistemática y continúa, y;

Que con el objeto de atender los deberes de la Ley General de Protección de Datos en Posesión de Sujetos Obligados y Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo y del marco normativo aplicable a la materia, en una Sesión Extrordinaria del Comité de Transparencia del Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública, celebrada el día miercoles 05 de octubre de 2022, se aprobó el Acuerdo 02/SEO/2022, por el que se emite el "Documento de Seguridad para la Protección de Datos Personales del Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública".
Derivado de lo anterior, en la Sesión Extraordinaria, celebrada el 05 de octubre de 2022, el Comité de Transparencia del **SESESP** aprobó el;

El "Documento de Seguridad para la Protección de Datos Personales de la Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública".

Capítulo I

Objeto y Ámbito de Aplicación

Primero. - El presente apartado normativo del **Documento de Seguridad** para la Protección de Datos Personales del Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública, es de observancia obligatoria para todas las personas servidoras públicas de este Organismo Público Descentralizado y tiene por objeto establecer las directrices y actividades para la generación de cada uno de los elementos que conforman el

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

Documento de Seguridad para la Protección de los Datos Personales en Posesión de las **Áreas** de este Sujeto Obligado.

Capítulo II
Disposiciones Generales

Segundo. - Para efectos del presente apartado normativo del **Documento de Seguridad** para la Protección de Datos Personales del Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública, se entenderá, en singular o en plural, por:

I. **Activos**: Todo elemento de valor para el Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública, involucrado en el tratamiento de datos personales, entre ellos, las bases de datos, el conocimiento de los procesos, el personal, el hardware, el software, los archivos.

II. **Análisis de Riesgos**: El estudio de las causas de las posibles amenazas y probables eventos no deseados, así como los daños y consecuencias que éstas puedan producir en la información en posesión del Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública.

III. **Áreas**: Las Unidades Administrativas del Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública, que traten o puedan tratar datos personales.

IV. **Área Administrativa:** Unidad Administrativa del **SESESP**, con fundamento en el Artículo 9 de la Ley que Crea el Organismo Público Descentralizado Denominado Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública.

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

VI. **Datos Personales Sensibles**: Aquellos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datospersonales que puedan revelar aspectos de origen racial, étnico, estados de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

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

VIII. **Encargado**: La persona física o moral, del ámbito público o privado, ajeno al Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública que solo o conjuntamente con otras, trate datos personales a nombre y por cuenta del Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública.

IX. **IDAIPQROO**: El Instituto de Acceso a la Información Pública y Protección de Datos Personales de Quintana Roo.

X. **Incidente**: Cualquier violación a las medidas de seguridad físicas, técnicas o administrativas del SESESP, que afecte la confidencialidad, la integridad o la disponibilidad de los datos personales.

XI. **Inventario**: El inventario de datos personales y sistemas de tratamiento cuya finalidad es tener el control documentado de los tratamientos que realizan las áreas del SESESP, realizado con orden y precisión.

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

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

XIV. **Lineamientos**: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

XV. **Medidas de Seguridad**: El conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger la información en posesión del Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública.

XVI. **Medidas de Seguridad Físicas**: Las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información.

XVII. **Remisión**: Toda comunicación de datos personales realizada exclusivamente entre el Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública y el Encargado, dentro o fuera del Estado y del territorio mexicano.

XVIII. **Sistema de Gestión**: El conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.

XIX. **SESESP**: El Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública.

XX. **Comité**: El Órgano colegiado al que hacen referencia los artículos 43 de la Ley General de Transparencia y Acceso a la Información Pública y 96 de la Ley Protección de Datos Personales en Posesión de Sujetos Obligados Para el Estado de Quintana Roo.

XXI. **Transferencia**: Toda comunicación de datos personales dentro o fuera del Estado de Quintana Roo y el territorio mexicano, realizada a personas distinta del titular, del Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública, o del encargado.

XXII. **Tituiar**: Persona física a quien corresponden los datos personales.

XXIII. **Tratamiento**: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso,

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

XXIV. **UTAIPyPDP**: Unidad de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, instancia a la que hace referencia el artículo 85 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y 97 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Quintana Roo.

XXV. **Vulnerabilidad**: La circunstancias o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño, y

XXVI. **Vulneración de Seguridad**: El incidente de seguridad que afecta a los datos personales en cualquier fase de su tratamiento.

Capítulo III

Del Control y Actualización del Documento de Seguridad

Tercero. - De conformidad con lo establecido en el artículo 35 de la **Ley General**, y el 37 de la **Ley Estatal**, el **Documento de Seguridad** debe contener:

I. El inventario de datos personales y de los sistemas de tratamiento;
II. Las funciones y obligaciones de las personas que traten datos personales;
III. El análisis de riesgos;
IV. El análisis de brecha;
V. El plan de trabajo;
VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
VII. El programa general de capacitación.

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

Cuarto. – Con fundamento en el artículo 36 de la **Ley General**, y el 38 de la **Ley Estatal**, el **Documento de Seguridad** deberá ser actualizado por la **UTAIPyPDP** en coordinación con las **Áreas** respectivas del **SESESP**, cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que se 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.

Capítulo IV

Del Inventario de Datos Personales

Quinto. - La **UTAIPyPDP** en coordinación con las **Áreas** respectivas del **SESESP** que traten **datos personales**, deberán elaborar un inventario de datos personales y de los sistemas de tratamiento datos personales y de sistemas de tratamiento, el cual contendrá lo siguiente:

I. El catálogo de medios físicos y electrónicos a través de los cuales se obtienen los datos personales;
II. Las finalidades de cada tratamiento de datos personales;
III. El catálogo de los tipos de datos personales que se trate, indicando si son sensibles o no;
IV. El catálogo de formatos de almacenamiento, así como la descripción general de la ubicación física y/o electrónica de los datos personales;
V. La lista de servidores públicos que tiene acceso a los sistemas de tratamiento;
VI. En su caso, el nombre completo o denominación o razón social del encargado y el instrumento jurídico que formaliza la prestación de los servicios que brinda al responsable;
VII. En su caso, los destinatarios o terceros receptores de la transferencia que se efectúan, así como las finalidades que justifican éstas, y

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

VIII. Fundamento legal para su tratamiento.

Anexo 2 ***Inventario de Datos Personales y de los Sistemas de Tratamiento.***

Sexto. - En la elaboración del inventario, la **UTAIPyPDP** y las **Áreas** deberán considerar conforme al artículo 33, Fracción I, de la **Ley General**, y el artículo 34, Fracción I, de la **Ley Estatal**, el ciclo de vida de los datos personales conforme lo siguiente:

I. La obtención de datos personales.
II. El almacenamiento de los datos personales.
III. El uso de los datos personales conforme su acceso, manejo, aprovechamiento, monitoreo y procesamiento, incluyendo los sistemas físicos y/o electrónicos utilizados para tal fin;
IV. La divulgación de los datos personales considerando las remisiones y transferencias que, en su caso, se efectúen;
V. El Bloqueo de los datos personales, en su caso, y
VI. La cancelación, supresión o destrucción de los datos personales.

La **UTAIPyPDP** y las **Áreas** deberán identificar el riesgo inherente de los **Datos Personales**, contemplando su ciclo de vida y los activos involucrados en su tratamiento, como podrían ser hardware, software o cualquier otro recurso humano o material que resulte pertinente considerar.

Séptimo. - A efecto de dar cumplimiento a lo establecido en el artículo 33, Fracción III y V, de la **Ley General**, y el artículo, 34 Fracción III y V de la **Ley Estatal**, la **UTAIPyPDP** pondrá a disposición de las **Áreas** del **SESESP** que posean datos personales el formato de **Inventario de Datos Personales** y de los Sistemas de Tratamiento (**Anexo 1**) para la debida requisición de cada uno de los rubros contenidos en el mismo, conforme a los siguientes criterios:

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

Rubros	Criterios
1.- Nombre del sistema	El **Área** tratante de los datos personales deberá precisar el nombre del sistema en donde se encuentren alojados éstos.
2.- Formato de almacenamiento	El **Área** deberá seleccionar una de las siguientes opciones: **Físico:** Para aquellos datos contenidos en registros manuales, impresos o visuales. **Electrónico:** Para aquellos datos que se encuentran contenidos en dispositivos informáticos o en una herramienta tecnológica específica para su acceso, recuperación o tratamiento. **Mixto:** Aquellos datos que se encuentran contenidas en ambas modalidades (físico y electrónico).
3.- Finalidades del tratamiento de datos personales	Precisar el propósito del tratamiento de los datos personales, los cuales deberán estar relacionados con las atribuciones conferidas al área tratante en la normatividad aplicable.
4.- Fundamento jurídicos para el tratamiento	Se requiere señalar los artículos, numerales, fracciones, apartados e incisos, así como el nombre de la normativa que faculta al área para llevar a cabo el tratamiento de los datos personales.
5.- Datos personales que se recaban	Enlistar los datos personales que se recaban en el sistema, precisando aquellos que sean de carácter sensible.

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

Rubros	Criterios
6.- Descripción general de la ubicación de los datos personales.	Señalar la ubicación física o electrónica en donde se alojan los datos personales, precisando la oficina, número de archivero, almacén, bodega nombre del programa, nombres de las carpetas en donde se encuentran los datos y las computadoras de las personas servidoras públicas tengan acceso a éstos.
7.- Realiza transferencias de datos personales.	Seleccionar la opción según corresponda "Sí" o "No".
8.-Destinatarios o receptores de las transferencias	En caso de haber seleccionado la opción "Sí" en el rubro que antecede, se debe precisar las personas físicas o morales, nacionales o internacionales receptores de los datos personales. Este apartado deberá permanecer vacío en caso de haber seleccionado la opción "No" en el rubro número 7.
9.-Finalidades que justifican las transferencias	Precisar las razones por las cuales se transfirieron los datos a los destinatarios citados en el rubro 8. Este apartado deberá permanecer vacío en caso de haber seleccionado la opción "No" en el rubro número 7.
10.-Listado de servidores públicos que tienen acceso al sistema	Colocar el nombre, cargo y área de adscripción de las personas servidoras públicas que tienen acceso al sistema

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

Rubros	Criterios
11.-Nombre del encargado que trata datos por cuenta y a nombre del **SESESP**	Precisar el nombre de la persona física o moral, pública o privada ajena al **SESESP**, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta de este organismo público descentralizado. Este apartado deberá permanecer vacío si no existe una relación con un encargado.
12.-Instrumento Jurídico que formaliza la prestación de los servicios que brinda el **SESESP**	Precisar el nombre del instrumento jurídico, así como la fecha de celebración de este, a través del cual se formaliza la relación entre el **encargado** y el **SESESP.**
13.- Nombre del Proceso	Esta información será requisitada por el **Área Administrativa** responsable del Sistema Físico y/o Electrónico que contenga datos personales, en caso de contar con dicha información, de lo contrario la requisitará la **UTAIPyPDP** en concordancia con el inventario de procesos institucional.
14.- Nombre de (los) Procedimiento(s)	Esta información será requisitada por el **Área Administrativa** responsable del Sistema Físico y/o Electrónico que contenga datos personales, en caso de contar con dicha información, de lo contrario la requisitará la **UTAIPyPDP** en concordancia con el inventario de procesos institucional.

Las **Áreas** del **SESESP**, deberán requisitar el formato de **Inventario de Datos Personales** y de los Sistemas de Tratamiento (Anexo 1) por cada uno de los sistemas en donde recaben y traten datos personales.

Octavo. - Anualmente, la **UTAIPyPDP** requerirá a las **Áreas** del **SESESP** la actualización de los formatos de Inventario, y en su caso, la inclusión y/o

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

eliminación de los sistemas que correspondan. Por lo que, como resultado de dicha actividad se actualizará el **Inventario de Datos Personales** y de los Sistemas de Tratamiento (Anexo 2).

Capítulo V

De las Funciones y Obligaciones de las Personas que tratan Datos Personales

Noveno. - De conformidad con el artículo 33 fracción II, de la **Ley General**, y el artículo 34, Fracción III, de la **Ley Estatal**, las personas servidoras públicas de las **Áreas** del **SESESP** que, en el ejercicio de sus funciones, traten datos personales tendrán, de manera enunciativa más no limitativa las siguientes funciones y obligaciones:

I. Tratar los datos personales que obren en su poder, conforme a las atribuciones de su área de adscripción observando los principios de licitud, lealtad, consentimiento, información, proporcionalidad, finalidad, calidad y responsabilidad;
II. Guardar confidencialidad respecto de los datos personales tratados, dicha obligación subsistirá aún después de finalizar las relaciones laborales con el **SESESP** y sin menoscabo de lo establecido en las disposiciones de acceso a la información pública;
III. Acatar las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que emitan las áreas competentes para tal efecto en documentos normativos del **SESESP**;
IV. Informar a la **UTAIPyPDP**, en caso de que se presente una vulneración u ocurra un incidente a la seguridad de los datos personales;
V. Requisitar el formato de Inventario de Datos Personales, conforme a lo establecido en el numeral Séptimo del presente documento y con el acompañamiento de la **UTAIPyPDP**;
VI. Solicitar a la **UTAIPyPDP**, la generación de los Avisos de Privacidad que, en su caso, requiera con la finalidad de ponerlos a disposición de los titulares de datos personales;

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, Mexico.

VII. En caso de requerir servicios que impliquen el tratamiento de datos personales por un tercero, informar a la **UTAIPyPDP** y a el **Área Administrativa** para que, en el ámbito de sus respectivas competencias, se efectúe la formalización de la relación jurídica entre el **Encargado** y el **SESESP**. Cuando el **Encargado** solicite una autorización para subcontratar servicios que impliquen el tratamiento de datos personales, informar a la **UTAIPyPDP** y al **Área Administrativa**, para que procedan conforme a sus atribuciones a efecto de deliberar lo conducente respecto de la subcontratación y, en su caso, autorizar y formalizar la misma mediante el instrumento jurídico que resulte aplicable conforme al marco normativo.

VIII. En caso de requerir transferir o remitir datos personales en los ámbitos estatal, nacional e internacional, informar a la **UTAIPyPDP**, para que procedan conforme a sus atribuciones en cuanto a la formalización de la relación jurídica entre el responsable y el receptor mediante la suscripción del instrumento jurídico idóneo, de conformidad con la normatividad que resulte aplicable al **SESESP**, que permita demostrar el alcance del tratamiento de los datos personales así como las obligaciones y responsabilidades asumidas por las partes, y;

IX. Suprimir los datos personales objeto de tratamiento una vez que se extingan las causas de su tratamiento o previa instrucción de la o el superior jerárquico, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales conforme a la normatividad aplicable.

Décimo. - Corresponde a la **UTAIPyPDP** y a el **Área Administrativa** con el **Área** requirente, verificar la formalización de la relación jurídica que, en su caso, se efectúe entre el **Encargado** y el **SESESP**, a través del instrumento jurídico idóneo, de conformidad con la normativa que resulte aplicable, y que permita acreditar su existencia, alcance y contenido.

En caso, de que el **Encargado** solicite autorización para llevar a cabo una subcontratación, deberán deliberar lo conducente respecto de la misma y, en su caso, autorizarla y formalizarla mediante un contrato o cualquier otro instrumento jurídico que resulte aplicable conforme al marco normativo del **SESESP.**

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

Décimo primero.- Corresponde a la **UTAIPyPDP**, establecer las medidas de seguridad de carácter administrativo y físico para la protección de los activos involucrados en el tratamiento de datos personales, que permitan protegerlos contra daño, perdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, de conformidad con lo dispuesto en la **Ley General** y **Ley Estatal**, en coordinación con todas las **Áreas** del **SESESP.**

Por lo que hace a las medidas de seguridad físicas, todas las **Áreas** del **SESESP** deberán implementar 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, considerarán las siguientes actividades:

I. Prevenir el acceso no autorizado al perímetro del **SESESP**, sus instalaciones físicas, áreas críticas, recursos e información;
II. Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas, recursos e información del **SESESP**;
III. Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir del **SESESP**, y
IV. Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Décimo segundo. - Todas las **Áreas** del **SESESP**, por medio de la **UTAIPyPDP**, establecerán los procedimientos para la conservación y supresión de los datos personales.

Décimo tercero. - Corresponde al **Área Administrativa**;

I. Establecer y mantener las medidas de seguridad de carácter técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, en coordinación con todas las áreas del **SESESP** que traten **Datos Personales**.
II. Dentro del 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) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software hardware del **SESESP**, y
c) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

III. Cerciorarse en coordinación con la **UTAIPyPDP** de que los servicios, aplicaciones e infraestructura de cómputo y otras materias para el tratamiento de datos personales a los que se adhiera el **SESESP**, cumplan con las disposiciones establecidas en la **Ley General** y la **Ley Estatal**.

Capítulo VI

Del Análisis de Riesgos, el Análisis de Brecha y el Plan de Trabajo.

Décimo cuarto. – El **Área Administrativa** y **UTAIPyPDP**, en el ámbito de sus respectivas atribuciones, realizarán una matriz de riesgos aplicada a las **Áreas** del **SESESP** que tratan datos personales, de la cual surgirá el documento de **Análisis de Riesgos** que contendrá por lo menos, lo siguiente:

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
II. El valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida;
III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida;
V. El riesgo inherente a los datos personales tratados, considerando los activos, las amenazas y las vulnerabilidades;
VI. La sensibilidad de los datos personales tratados;

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

VII. El desarrollo tecnológico;
VIII. Las posibles consecuencias de una vulneración para los titulares;
IX. Las transferencias de datos personales que se realicen;
X. El número de titulares;
XI. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
XII. 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.

Anexo 3 *Análisis de Riesgos.*

Para dar cumplimiento al artículo 34, fracción IV, de la **Ley Estatal,** se deberá realizar un análisis de riesgos de los datos personales tratados considerando lo siguiente:

Medidas de seguridad administrativas.	
Punto	**Descripción**
A. Declaración de confidencialidad:	Realizar esta declaración que será puesta a disposición del personal que interviene en el tratamiento de datos personales para que estén informados de los deberes y medidas de seguridad que deben tomar en consideración en sus actividades relacionadas con dichos tratamientos.
B. Listado de personal:	Elaborar un documento que contenga la relación del personal que interviene en el tratamiento de datos personales, en donde se incluya nombre, cargo, funciones en el tratamiento y obligaciones en materia de datos personales, por cada tratamiento.
C. Clasificación de los archivos físicos:	Identificar o incluir la base de datos en soporte físico en el Catálogo de Disposición Documental para tener control del ciclo de vida a que deben estar sujetos los archivos administrativos

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

D. Clasificación de los archivos electrónicos:	Identificar y etiquetar las bases de datos en soporte electrónico con el nombre del Tratamiento de Datos Personales conforme al Inventario reportado por las **Áreas Administrativas.**
E. Capacitación:	El personal involucrado en el tratamiento de los datos personales deberá asistir a los cursos de capacitación implementados por el **Comité de Transparencia** en el Programa Anual de Capacitación.
F. Bitácora de vulneraciones:	Implementar un control informativo en donde se reporten los tipos de vulneraciones con los siguientes datos: fecha y lugar en donde se produjo, nombre y cargo de quien notifica la incidencia, nombre y cargo de la persona a la que se le comunica, y las medidas que se implementaron para subsanar la misma. Toda vulneración deberá notificarse, también, a la Unidad de Transparencia para que tome las acciones pertinentes Si la vulneración trasciende a una posible afectación directa de los titulares de los datos personales, especialmente en sus derechos patrimoniales o en su esfera más íntima (datos sensibles), se deberá notificar a los titulares afectados para que tomen las medidas pertinentes para la defensa de sus derechos.
G. Depuración y borrado seguro del archivo físico:	Transferir y depurar el archivo físico de manera periódica, conforme a los plazos de conservación y parámetros dispuestos la normativa en materia.
H. Depuración y borrado seguro del archivo electrónico:	Borrar, de manera segura y permanente, las bases de datos o parte de ellas que se encuentren en archivo electrónico, en desuso o que hayan cumplido su finalidad o el tiempo de conservación dispuesto para el archivo administrativo.

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

	Solicitar al **Área Administrativa** de la Información que proporcione un programa para el borrado integral de la información, o en su defecto, reinicio de los equipos o medios de almacenamiento a los valores de origen. Además, para la depuración y borrado seguro de las bases de datos electrónicas, se deberá levantar un acta, signada por el titular del área y remitirse copia de la misma a la **UTAIPyPDP.**
I. Responsable de seguridad:	Designar un responsable de seguridad para coordinar y verificar las medidas de seguridad establecidas en el Documento de Seguridad.
J. Transferencias:	Realizar transferencias con las medidas de confidencialidad necesarias, enviar la información en sobre cerrado y con la leyenda de "confidencial" o en archivos electrónicos encriptados.

Medidas de seguridad físicas.	
Punto	**Descripción**
A. Cuidado de los bienes informáticos:	Mantener en buen estado el bien informático que le haya sido asignado y no abrir los equipos o bien, introducir en ellos cualquier tipo de instrumento o software que no sean los apropiados para el trabajo y que no hayan sido validados por el **Área Administrativa**, tampoco alterar el orden de los cables conectados.
B. Prevenir accesos no autorizados:	Prevenir que el acceso a las bases de datos o a la información, así como a los recursos que las contengan, se realice únicamente por usuarios identificados y autorizados por el área.
C. No instalar equipos ajenos:	Abstenerse de instalar equipos de cómputo que no sean propiedad de la **SESESP** sin permiso del **Área Administrativa**. Los usuarios que requieran hacer uso de la red interna de **SESESP** deben usar solamente las direcciones IP asignadas por el área administrativa

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, Mexico.

	correspondiente. En caso de requerir conectar un dispositivo de almacenamiento de información (p. ej. USB, disco duro portátil, etcétera) al equipo del usuario, éste debe ser revisado previamente por el antivirus.
D. Archivero con candado:	Resguardar las bases de datos en archivo físico en un archivero con candado o con llave de seguridad, cuyo acceso sólo será permitido al personal autorizado.

Décimo quinto. – El **Área Administrativa**, conforme a sus respectivas atribuciones en conjunto con la **UTAIPyPDP** realizarán un análisis de brecha, el cual contendrá por lo menos, lo siguiente:

I. Las medidas de seguridad existentes y efectivas;
II. Las medidas de seguridad faltantes, y
III. La existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.

Anexo 4 *Análisis de Brecha*.

Con relación al artículo 34, fracción V de la **Ley Estatal** para la realización del análisis de brecha el responsable deberá considerar lo siguiente:

I. Las medidas de seguridad existentes y efectivas;
II. Las medidas de seguridad faltantes, y
III. La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

Estado Actual	Expectativa a futuro	Brecha	Mejorar.

Por lo cual, se deberá en caso de detectar;

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

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

El análisis de brecha es de naturaleza diagnóstica y contribuye a conocer las áreas de oportunidad por cada tratamiento. A su vez, esta información da sustento a las políticas y mecanismos institucionales en materia de protección de datos personales que se han aprobado por el Comité de Transparencia para atenderlas de manera paulatina y en coordinación con cada una de las áreas:

Ciclo	Fases	Pasos	Objetivo Específicos
Planificar	Planear el Sistema de Gestión de Datos Personales	1. Alcance y objetivos 2. Política de gestión de datos personales. 3. Funciones y obligaciones de quienes traten datos personales. 4. Inventario de datos personales. 5. Análisis de riesgos de los datos personales. 6. Identificación de las medidas de seguridad y análisis de brecha	Definir los objetivos, políticas, procesos y procedimientos relevantes del Sistema de Gestión de Datos Personales para gestionar los riesgos de los datos personales, con el fin de cumplir con la legislación sobre protección de datos y obtener resultados acordes con las políticas y objetivos generales de la organización.
Hacer	Implementar y operar el Sistema de Gestión de Datos Personales	7. Implementación de las medidas de seguridad aplicables a los datos personales.	Implementar y operar las políticas, objetivos, procesos, procedimientos y controles o mecanismos del Sistema de Gestión de Datos Personales, considerando indicadores de medición.

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

Ciclo	Fases	Pasos	Objetivo Específicos
Verificar	Monitorear y revisar el Sistema de Gestión de Datos Personales	8. Revisiones y auditoría	Evaluar y medir el cumplimiento del proceso de acuerdo con la legislación de protección de datos personales, la política, los objetivos y la experiencia práctica del Sistema de Gestión de Datos Personales, e informar los resultados a la Unidad de Transparencia.
Actuar	Mejorar el Sistema de Gestión de Datos Personales	9. Mejora continua y Capacitación.	Para lograr la mejora continua se deben adoptar medidas correctivas y preventivas, en función de los resultados obtenidos de la revisión por parte de la Alta Dirección, las auditorías al Sistema de Gestión de Datos Personales y de la comparación con otras fuentes de información relevantes, como actualizaciones regulatorias, riesgos e impactos organizacionales, entre otros. Adicionalmente, se debe considerar la capacitación del personal.

Décimo sexto. – El **Área Administrativa**, conforme a sus respectivas atribuciones, en conjunto con la **UTAIPyPDP** y con la previa aprobación

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

del **Comité**, elaborarán un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Lo anterior, se realizará tomando en consideración los recursos asignados, el personal, y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes, para lo cual se requerirá de la participación del **Área Administrativa**.

Anexo 5 *Plan de Trabajo.*

De conformidad con lo dispuesto en el artículo 34, Fracción VI, de la **Ley Estatal**, el responsable deberá elaborar un plan de trabajo que defina las acciones a implementar de acuerdo con el resultado del análisis de riesgos y del análisis de brecha, priorizando las medidas de seguridad más relevantes e inmediatas a establecer.

Lo anterior, considerando los recursos designados; el personal interno y externo en su organización y las fechas compromiso para la implementación de las medidas de seguridad nuevas o faltantes, para dar cumplimiento al parrafo anterior, se deberá realizar lo siguiente:

I. Promover e impulsar la capacitación en materia de protección de datos personales a todos los sujetos responsables para abatir la falta de conocimiento por parte del personal de nuevo ingreso.
II. Identificar necesidades de capacitación en temas específicos en la implementación de la **Ley General y Ley Estatal**, como lo pueden ser: Obligaciones de la protección de datos personales; elaboración de avisos de privacidad y establecimiento de medidas de seguridad.
III. Aprobar el Programa General de Capacitación.
IV. Proponer la implementación de políticas de traslado seguro de la información en la cual se contienen datos personales mediante medidas de seguridad que eviten la vulneración de la información.
V. Impulsar la generación de procesos de digitalización de información que contiene datos personales.

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

VI. Sensibilizar sobre la importancia de la generación de copias de respaldo de la información que contiene datos personales para Documento de Seguridad minimizar el posible daño por pérdida de estos por razones de causas naturales o casos fortuitos.
VII. Actualizar el inventario de datos personales para la posible detección de nuevos tratamientos o la modificación de estos.
VIII. Promover la revisión periódica de las medidas de seguridad a efecto de identificar posibles deficiencias en sus procesos de implementación; para lo cual el sujeto responsable remitirá, por lo menos una vez al año, un informe al responsable designado conforme al art. 97 de la **Ley Estatal,** que dé cuenta de esta revisión.

En relación con lo anterior, a continuación, se presenta el Plan de Trabajo a desarrollarse:

ACCIÓN	ENCARGADO	TEMPORALIDAD
1	**UTAIPyPDP**	Permanente
2	**UTAIPyPDP**	Permanente
3	Comité de Transparencia	Anualmente
4	**UTAIPyPDP**	Permanente
5	Área competente de archivo	Anualmente
6	**UTAIPyPDP** y Área Administrativa	Permanente
7	**UTAIPyPDP**	Anualmente
8	Responsable designado conforme al Art. 97 de la **Ley estatal** y Sujetos Responsables	Permanente

Capitulo VII

De los Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad

Décimo séptimo. – La **UTAIPyPDP**, conforme a sus respectivas atribuciones en coordinación con las **Áreas** del **SESESP**, que realicen o puedan realizar tratamiento de datos personales, deberán realizar

mecanismos de monitoreo y revisión de las medidas de seguridad que protegen datos personales de manera periódica, conforme a lo siguiente:

I. Los nuevos activos que se incluya la gestión de riesgos;
II. Las modificaciones necesarias a los activos, como podría ser el cambio o migración tecnológica, entre otras;
III. Las nuevas amenazas que podrían estar activas dentro y fuera del **SESESP** y que no han sido valoradas;
IV. La posibilidad de que las vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes;
V. La Vulnerabilidad identificada para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelvan a surgir;
VI. El cambio en el impacto o consecuencia de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgos, y
VII. Las Vulnerabilidades que se presenten y las Vulneraciones de seguridad ocurridas.

Aunado a lo anterior, las **Áreas** en función a sus atribuciones del **SESESP**, deberán contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

Anexo 6 *Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad.*

El proceso general para el establecimiento, actualización, monitoreo y revisión de los mecanismos y medidas de seguridad; relacionadas al análisis de riesgo, se deberán realizar con el fin de revisar las medidas de seguridad implementadas para la protección de los datos personales recabados e informar, en los meses de enero y julio al responsable designado conforme al Articulo 97 de la **Ley Estatal**. Así mismo, el responsable designado podrá solicitar al Comité de Transparencia la aprobación de medidas, recomendaciones o criterios a los sujetos responsables, con el objeto de fortalecer las acciones implementadas para el adecuado tratamiento de los datos personales.

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

Tipos de Medidas de Seguridad	Descripción
Administrativas:	Son las políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel institucional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales:
Física:	Son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. Algunas de las actividades que se deben considerar son las siguientes: **1.** Prevenir el acceso no autorizado a las instalaciones físicas del SESESP; Para lo anterior, se deberá realizar algún acuerdo, convenio o en su caso contrato de prestación de servicios de Seguridad y vigilancia privada, con la Secretaría de Seguridad Pública con el fin de obtener vigilancia, protección a instalaciones, bienes y personas en el inmueble que ocupa el SESESP, es decir, resguardan las instalaciones, recursos e información las 24 horas los 365 días del año. **2.** Proveer a los equipos que almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad. Ademas de : **3.** Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; El acceso a la base de datos es exclusivo para el personal adscrito al SESESP. **4.** Revisar la configuración de seguridad en la operación, desarrollo y mantenimiento del

	software y hardware; Se realizan constantemente respaldos de la información. **5.** Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales. Se cuenta con protección Firewall y los antivirus propios de cada marca.

Esto deberá observarse durante todo el ciclo de vida de los datos personales, desde su obtención hasta su eliminación. Se deberán monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, con fundamento en el Articulo 97 de la **Ley Estatal**:

Capitulo VIII

Del programa de capacitaciones en materia de Protección de Datos Personales

Décimo octavo. – La **UTAIPyPDP**, previa aprobación del **Comité**, deberá diseñar e implementar un programa a corto, mediano y largo plazo que tengan por objeto capacitar a las personas servidoras públicas de **SESESP**. Para el diseño e implementación de los programas de capacitación, se deberá tomar en cuenta lo siguiente:

I. Los requerimientos y actualizaciones del sistema de gestión;
II. La legislación vigente en materia de protección de datos personales y las mejores prácticas para el tratamiento de éstos;
III. Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales, y;
IV. Las herramientas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

Anexo 7 *Programa de Capacitación*

Programa General de Capacitación en materia de datos personales, a fin de dar cumplimiento a esta obligación, **el SESESP**, a través del **Comité de Transparencia**, deberá aprobar anualmente el Programa de Capacitación Institucional que al efecto someta a consideración de este colegiado la Unidad de Transparencia, el cual deberá contemplar la materia de datos personales y, prever, al menos los temas siguientes:

No.	Tema
1	Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
2	Principios que regulan el tratamiento de datos personales, deberes y obligaciones de los sujetos responsables.
3	Inventario de Datos Personales.
4	Elaboración de Avisos de Privacidad (integral y simplificado).
5	Medidas de Seguridad orientadas a la Protección, Seguridad y Confidencialidad en el Tratamiento de Datos Personales.

En su integración deberán considerarse diversas fechas para la impartición de los cursos, los roles del personal involucrado en el tratamiento de datos personales y las áreas a las que estos corresponden.

Dicho programa deberá ser difundido por responsable designado conforme al artículo 97 de la **Ley Estatal,** a todos el personal adscrito o responsables del manejo de Datos Personales del SESESP.

El Programa de Capacitación podrá prever la impartición de cursos a través del personal con que cuenta la Unidad de Transparencia, así como de aquella proporcionada por el IDAIPQROO o cualquier otra instancia del sector público o privado.

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

Capitulo IX

De los Deberes y Vulneraciones a la Seguridad

Décimo noveno. – El **Área Administrativa**, implementará sistemas de detección y/o registro de alertas de seguridad que adviertan respecto de anomalías o cambios no deseados en los activos del **SESESP**.

Las alertas de seguridad podrán ser manuales o automatizadas y originarse a través de diversas fuentes tales como: los titulares de los datos personales, usuarios de los sistemas de tratamiento, provenientes o de proveedores de servicios de telecomunicaciones, medios masivos de comunicaciones o sitios web especializados.

Conforme a lo anterior, el **Área Administrativa** en el ámbito de sus respectivas competencias, deberán asegurarse de que el **SESESP**, cuente al menos con los siguientes tipos de alertas:

Entorno	Tipo de alerta
Para entorno físico	• Alarmas para desastres naturales como incendios o terremotos • Alarmas contra robo o intrusos en las instalaciones • Alertas del personal de vigilancia o a través de circuito cerrado de televisión. • Aviso de desaparición o extravío de equipos de cómputo, medios de almacenamiento documentos. • Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento físico.
Para entorno electrónico	• Notificaciones sobre softwares maliciosos o vulnerabilidades técnicas descubiertas • Alertas de sistemas automatizados como firewalls, antivirus, filtros de contenido, sistemas de detección de intrusos o gestores de seguridad de la información • Anomalías o accesos no autorizados identificados en bitácoras de los sistemas de tratamiento automatizados, medios de almacenamiento y equipos de cómputo.

Vigésimo. - De manera enunciativa más no limitativa, se entenderá como vulneraciones de seguridad a los incidentes que afectan los datos personales en cualquier fase del tratamiento de los mismos, tales como; los siguientes:

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

Vigésimo primero. – Las personas servidoras públicas del **SESESP** que tengan acceso datos personales, tendrán la obligación de notificar, de manera inmediata, al o la superior jerárquico y a la **UTAIPyPDP**, de cualquier incidente detectado, debiendo notificar mediante escrito dentro de los siguientes tres días hábiles a que tuvo conocimiento, al menos, lo siguiente:

I. La información de la persona que ha detectado el incidente tales como nombre, extensión, área de adscripción y correo electrónico institucional;
II. La hora y fecha de la identificación de la vulneración;
III. La descripción de las circunstancias generales en torno a la vulneración; tales como localización del incidente, tipo de sistema de tratamiento (físico, automatizado o mixto), nombre del responsable del sistema de tratamiento y descripción de lo sucedido;
IV. Los datos personales comprometidos;
V. Las recomendaciones dirigidas que, en su caso, se puedan adoptar para proteger los datos personales;
VI. Las acciones correctivas realizadas que, en su caso, se hayan llevado a cabo, y
VII. Cualquier otra información y documentación que consideré conveniente hacer del conocimiento.

Vigésimo segundo. - Una vez que la **UTAIPyPDP** reciba el escrito citado en el numeral que antecede, en coordinación con el **Área Administrativa**,

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

deberán realizar una investigación sobre el incidente, con la finalidad de determinar el alcance de la afectación a los datos.

En caso de que un incidente afecte de forma significativa los derechos patrimoniales o morales del titular, la **UTAIPyPDP**, deberá informar lo conducente tanto al titular como al **IDAIPQROO**, en un plazo máximo de setenta y dos horas, en los términos que fijen los Lineamientos, la **Ley General** y **Ley Estatal.**

Vigésimo tercero. – Posterior a la investigación y, con independencia del tipo de incidente de que se trate, las áreas en donde se haya presentado éste, en coordinación con el **Área Administrativa**, conforme a sus respectivas atribuciones, realizarán un plan de implementación de medidas de seguridad para mitigar el incidente y prevenir eventos de dicha naturaleza, mismo que deberá ser informado a la **UTAIPyPDP.**

Vigésimo cuarto. - Las **Áreas** del **SESESP** que traten datos personales, deberán elaborar una bitácora de los incidentes a la seguridad, la cual será requisitada por una persona servidora pública designada para tal efecto y debe contener por lo menos los siguientes datos:

I. La fecha en la que ocurrió el incidente;
II. La o las causas del incidente de la Información restringida;
III. El tipo de Información restringida que fue vulnerada, y
IV. Las acciones correctivas que, en su caso, se hayan implementado.

Dicha bitácora deberá ser informada a la **UTAIPyPDP**, dentro de los cinco días hábiles posteriores a la implementación de las acciones correctivas que se hayan implementado.

Capitulo X

De la Interpretación

Vigésimo quinto. - El **Comité de Transparencia** del **SESESP** será el encargado de interpretar el presente apartado normativo del **Documento de Seguridad** y de resolver cualquier asunto no previsto en el mismo.

Transitorios

PRIMERO. El presente apartado normativo del **Documento de Seguridad** entrará en vigor al día siguiente de su aprobación por el **Comité de Transparencia** de **SESESP**.

SEGUNDO. El apartado normativo del **Documento de Seguridad** deberá ser difundido a todo el personal a través del correo electrónico institucional y publicado en el sitio web institucional del **SESESP**.

TERCERO. Instrúyase a la **UTAIPyPDP** para que realice el acompañamiento a las **Áreas** respectivas del **SESESP**, en la elaboración o complementación y/o actualización de lo siguiente: Inventario de Datos Personales y de los Sistemas de Tratamiento; el Análisis de Riesgos; el Análisis de Brecha; el Plan de Trabajo; los Mecanismos de monitoreo y revisión de las medidas de seguridad y el Programa de Capacitación.

Ciudad de Chetumal, Quintana Roo, septiembre 2022.

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.

QUINTANA ROO
COBIERNO DEL ESTADO 2022|2027

COBIERNO DEL ESTADO
2022|2027

SESESP

SECRETARIADO EJECUTIVO DEL SISTEMA ESTATAL DE SEGURIDAD PÚBLICA

Calle 1 de mayo s/n con Tomas Aznar Barbachano
Colonia Proterritorio, C.P. 77086
Chetumal, Quintana Roo, México.