DOCUMENTO DE SEGURIDAD DEL SECRETARIADO EJECUTIVO DEL SISTEMA DE SEGURIDAD PÚBLICA DEL ESTADO DE TABASCO

ÍNDICE

CONTENIDO

INTRODUCCIÓN

En el presente documento se detallan las medidas de seguridad administrativas, físicas y técnicas con las que se contará en el SESESP para garantizar la debida protección de los datos personales a los que se les da tratamiento en las direcciones que los manejan.

Con este documento de seguridad se da cumplimiento al artículo 40 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco.

GLOSARIO DE TÉRMINOS

I. Aviso de Privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus Datos Personales, con el objeto de informarle los propósitos del tratamiento de los mismos;

II. Bases de Datos: Conjunto ordenado de Datos Personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;

III. 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. Durante dicho periodo, los Datos Personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la Base de Datos que corresponda;

IV. Comité de Transparencia: Organismo colegiado de carácter normativo constituido al interior de los Sujetos Obligados;

V. Cómputo en la Nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;

VI. Consejo Estatal: Consejo Estatal del Sistema Estatal de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, a que refiere el artículo 33 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco;

VII. Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;

VIII. 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 puede determinarse directa o indirectamente a través de cualquier información, siempre y cuando esto no requiera plazos, medios o actividades desproporcionadas;

IX. 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. De manera enunciativa más no limitativa, se consideran sensibles los Datos Personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

X. Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de Datos Personales;

XI. Días: Días hábiles;

XII. Disociación: El procedimiento mediante el cual los Datos Personales no pueden asociarse al Titular, ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;

XIII. Documento de Seguridad: 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;

XIV. Encargado: La persona física o jurídica colectiva, 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;

XV. Evaluación de Impacto en la Protección de Datos Personales: Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de Datos Personales, valoran los impactos reales respecto de determinado tratamiento de Datos Personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los Titulares, así como los deberes de los Responsables y encargados, previstos en la normatividad aplicable;

XVI. Fuentes de Acceso Público: Aquellas Bases de Datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, 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, conforme a las disposiciones establecidas por la presente Ley y demás normatividad aplicable;

XVII. Instituto: Instituto Tabasqueño de Transparencia y Acceso a la Información Pública;

XVIII. Instituto Nacional: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XIX. Medidas Compensatorias: Mecanismos alternos para dar a conocer a los titulares el Aviso de Privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;

XX. Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los Datos Personales;

XXI. Medidas de Seguridad Administrativas: Políticas y procedimientos para !a gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de Datos Personales;

XXII. 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, 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;

XXIII. 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 o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

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

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

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

XXIV. Plataforma Nacional: La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública;

XXV. Remisión: Toda comunicación de Datos Personales realizada exclusivamente entre el Responsable y Encargado, dentro o fuera del territorio mexicano;

XXVI. Responsable: Los Sujetos Obligados a que se refiere el artículo 1 de la presente Ley, que deciden y determinan los fines, medios y demás cuestiones relacionadas con determinado tratamiento de Datos Personales;

XXVII. Sistema Estatal: El Sistema Estatal de Transparencia, Acceso a la Información Pública y Protección de Datos Personales;

XXVIII. Sistema Nacional: El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XXIX. Supresión: La baja archivística de los Datos Personales conforme a la normatividad archivística aplicable, que resulte en la eliminación, borrado o destrucción de los Datos Personales bajo las Medidas de Seguridad previamente establecidas por el Responsable;

XXX. Titular: La persona física a quien corresponden los Datos Personales;

XXXI. Transferencia: Toda comunicación de Datos Personales dentro o fuera del territorio mexicano, realizada a persona distinta del Titular, del Responsable o del encargado;

XXXII. Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los Datos Personales, relacionadas 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, transferencia y en general cualquier uso o disposición de Datos Personales; y

XXXIII. Unidad de Transparencia: Instancia a la que hace referencia el Capítulo IV, del Título Segundo, de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco.

XXXIV. SESESP: Secretariado Ejecutivo del Sistema Estatal de Seguridad Pública.

INVENTARIO Y CATÁLOGO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO

1) Nivel de seguridad de los datos personales a los que se les da tratamiento en el SESESP:

Para mayor garantía de seguridad en los datos personales y en las bases de datos personales, físicas o electrónicas, donde se concentran los mismos, las medidas de seguridad que se implementarán corresponden a un nivel de seguridad **alto**, siempre garantizando la confidencialidad, integridad y disponibilidad de los datos personales, tal y como lo expresa la Ley.

2) Transferencias de los datos personales:

Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 3 fracción XIII, 124 y 128 de la Ley.

LAS FUNCIONES Y OBLIGACIONES DE LAS PERSONAS QUE TRATEN DATOS PERSONALES

Las direcciones, encargadas de tratar datos personales son las siguientes:

Dirección del Sistema Estatal de Información.

Dirección del Centro Estatal de Evaluación y Control de Confianza.

Las personas que desempeñan los puestos anteriormente mencionados, tienen como funciones y obligaciones las siguientes:

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

REGISTRO DE INCIDENCIAS

Las incidencias con datos personales que se produzcan vulnerarán la debida protección de los mismos, por lo tanto, es necesario que en las direcciones del SESESP en donde se de tratamiento a datos personales lleven a cabo un registro de las incidencias que comprometen la seguridad de los datos.

El registro de incidencias deberá contener, por lo menos, la fecha de la incidencia, el tipo, descripción, la persona quien la registra, persona a quien se la comunica y la o las consecuencias que tendrá esa incidencia. (Anexo 1)

El personal del SESESP que trate datos personales deberá de contar con el registro de incidencias, ya que quien identifique la incidencia será el encargado de registrarla y notificar a su superior inmediato, quien a su vez se encargará de notificar a la o las personas afectadas para que éste tome las precauciones debidas en caso de uso inadecuado de la información.

IDENTIFICACIÓN Y AUTENTICACIÓN

En la Dirección del Sistema Estatal de Información, es quien administra las bajas y altas de correos electrónicos del personal del SESESP, así como las sesiones en los equipos de cómputo.

El personal designado en la Dirección del Sistema Estatal de Información asigna usuarios y contraseñas, siendo estas últimas aleatorias y se exige que se modifiquen.

La reserva y confidencialidad de estas contraseñas queda bajo la responsabilidad de la persona a la que se le asignó la cuenta de usuario.

Por ningún motivo las cuentas y las contraseñas de los usuarios de los correos electrónicos y de los equipos de cómputo serán transferibles

CONTROL DE ACCESO Y GESTIÓN DE SOPORTE

En todo momento, las direcciones del SESESP que dan tratamiento a datos personales deberán tener un control de acceso a sus bases de datos personales físicas o electrónicas, en el cual establecerán medidas de seguridad que salvaguarden la confidencialidad e integralidad de la información resguardada.

[redacted]

ELIMINADO: cuatro renglones. Información Reservada. Artículo 121 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco. Su publicación pondría en riesgo la Vida de las personas que laboran en el SESESP y de la Seguridad Nacional y del Estado.

Año tras año las direcciones del SESESP deberán enviar la información física que contenga datos personales al Archivo del SESESP, el cual deberá de contar con las instalaciones y protección adecuada para el resguardo de la misma información.

El archivo del SESESP, por su parte, evitará en la medida de lo posible extraer información que contenga datos personales, esto con la finalidad de evitar el mal uso o la pérdida de la información.

COPIAS DE RESPALDO Y RECUPERACIÓN

[redacted]

ELIMINADO: cinco renglones. Información Reservada. Artículo 121 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco. Su publicación pondría en riesgo la Vida de las personas que laboran en el SESESP y de la Seguridad Nacional y del Estado.

Dichas copias de seguridad de la información física y electrónica deberán realizarse semanalmente y estarán bajo el resguardo de la persona que les da el tratamiento.

ANÁLISIS DE RIESGOS

De acuerdo a una matriz de análisis de riesgos aplicada a las direcciones del SESESP que dan tratamiento a datos personales, se consideran como vulneraciones comunes las siguientes:

a) Robo, extravío o copia no autorizada.
b) Destrucción no autorizada
c) Daños por situaciones fortuitas.

ANÁLISIS DE BRECHA

Las medidas de seguridad que se señalan en este documento de seguridad se pretende que queden asentadas y uniformes.

PLAN DE TRABAJO

El plan de trabajo para la protección de los datos personales que el SESESP llevará a cabo será cumplir con el proyecto de conformidad con lo previsto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco y las demás disposiciones que le resulten aplicables en la materia, que contará con los siguientes pasos:

1. Implementar medidas de seguridad físicas, administrativas y técnicas para la debida protección de los datos personales.
2. Conformar el documento de seguridad como lo requiere la Ley.
3. Llevar a cabo visitas de seguimiento y de verificación, esto con el objetivo de corroborar el cumplimiento de las obligaciones que marca la Ley.

LOS MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Las medidas de seguridad administrativas, físicas y técnicas serán de aplicación a todas las bases de datos personales que manejan las personas a cargo de las direcciones en la fracción V del presente documento, esto de acuerdo a sus funciones y obligaciones.

[redacted]

ELIMINADO: veintidos renglones. Información Reservada. Artículo 121 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco. Su publicación pondría en riesgo la Vida de las personas que laboran en el SESESP y de la Seguridad Nacional y del Estado.

PROGRAMAS DE CAPACITACIÓN Y ACTUALIZACIÓN

En caso de que en el transcurso del año se presente alguna modificación a la ley de la materia, surja alguna actualización en el tema o alguna de las Unidades Administrativas tenga la necesidad de capacitación, se solicitará la programación del curso.

ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD

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, e
IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.
V. Cuando surjan documentos, formatos, recomendaciones, etc. por parte del INAI para la mejora del documento de seguridad.

ANEXOS

Anexo 1

Registro de incidencias.

Fecha de la incidencia:	Número de incidencia:
Tipo de incidencia:	
Descripción detallada de la incidencia:	
Nombre y cargo de la persona que registra la incidencia:	
Nombre y cargo de la persona a quien se le comunica la incidencia:	
Consecuencias de la incidencia:	

Firma de quien registra la incidencia

_____

Firma de a quien se le comunicó la incidencia

_____