

Expediente OSFE/STYT/SOL/083/2024

Asunto: Acuerdo de Disponibilidad de la Información.

**SECRETARÍA TÉCNICA Y TRANSPARENCIA, DEL ÓRGANO SUPERIOR DE FISCALIZACIÓN DEL ESTADO.
VILLAHERMOSA, TABASCO, 11 DE NOVIEMBRE DE 2024.** -----

Visto. – El estado que guarda el expediente número **OSFE/STYT/SOL/083/2024**, formado con motivo de la solicitud de acceso a la información presentada a través de la Plataforma Nacional de Transparencia, el día 21 de octubre de 2024, a las 11:03 horas, por el Representante que dijo llamarse **"ADAN AUGUSTO MAY RODRIGEZ"** y registrada bajo el folio **270509400008324**, mediante la cual requirió:

"SOLICITO COPIA EN VERSION ELECTRONICA DEL DOCUMENTO DE SEGURIDAD QUE TODO SUJETO OBLIGADO DEBE POSEER DE ACUERDO A LO PREVISTO EN LA LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL ESTADO DE TABASCO, ASI COMO LOS ACUERDOS DE PRIVACIDAD ACTUALIZADOS." (sic)

Esta Secretaría Técnica y Transparencia (en adelante STYT), previo a la emisión del presente acuerdo, precisa lo siguiente:

- La *Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco* vigente, tiene por objeto establecer los principios, bases y procedimientos para garantizar el **Derecho de Acceso a la Información Pública (en adelante DAI por sus siglas)** en posesión de los Sujetos Obligados, que reciban y ejerzan recursos públicos o realicen actos de autoridad, en los órdenes estatal y municipal. Lo anterior, de conformidad con el artículo primero de la citada Ley¹.-----
- Ahora bien, conforme a la fracción VII, del numeral 3 de la Ley en comento, se define al **Derecho de Acceso a la Información Pública** como: "*la Prerrogativa que tiene toda persona para acceder a la información generada, obtenida, adquirida, transformada, creada, administrada o en poder de los Sujetos Obligados o de interés público*" (sic).-----
- De lo anterior, es de señalar que para ejercer dicho Derecho, las personas interesadas no necesitan acreditar ningún tipo de derecho subjetivo, interés legítimo o razones que motiven su pedimento,

¹ Ley de Transparencia y Acceso a la Información Pública.

"Artículo 1. La presente Ley es de orden público y de aplicación en todo el Estado, en materia de Transparencia y acceso a la Información Pública, en los términos previstos por el artículo 4º Bis de la Constitución Política local; y tiene por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de los Sujetos Obligados, que reciban y ejerzan recursos públicos o realicen actos de autoridad en el orden estatal o municipal." (sic)



lo que se traduce en que una persona no tendrá que acreditar su identidad, ni fundar y motivar su pedimento; por lo que, para efectos de poder hacer valerlo, el interesado podrá ejercerlo a través de una solicitud de acceso a la información pública, con el objeto de acceder a **todo archivo, registro o dato contenido en cualquier medio, documento o registro impreso, óptico, electrónico, magnético o físico que generen o posean los Sujetos Obligados** y que no hubiera sido clasificado como de acceso restringido (confidencial o reservado).- - - - -

- Por lo que, la aplicación e interpretación del DAI, se realizará bajo los principios establecidos en la *Constitución Política de los Estados Unidos Mexicanos*, la *Ley General de Transparencia y Acceso a la Información Pública*, los Tratados Internacionales de los que el Estado mexicano sea parte, la *Constitución Política del Estado Libre y Soberano de Tabasco*, y la *Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco*, favoreciendo en todo tiempo la protección más amplia a las personas, sin distinción alguna.- - - - -
- En ese tenor, los Sujetos Obligados se encuentran constreñidos a proporcionar la información relacionada estrictamente con el ejercicio de sus atribuciones, funciones o competencias², a cualquier persona, con la excepción de aquella considerada como información de acceso restringido en cualquiera de sus modalidades (reservada o confidencial), lo cual realizarán a través de la Unidad de Transparencia, quien es la responsable de recibir y tramitar toda solicitud de información que reciba un Sujeto Obligado atento al marco jurídico en la materia.- - - - -
- De conformidad con lo anterior, es necesario precisar que si bien los Sujetos Obligados están sometidos al principio de máxima publicidad de sus actos y obligados a respetar el derecho humano de acceso a la información pública, también lo es que su obligatoriedad de proporcionar información no comprende el procesamiento de la misma, ni el de presentarla conforme al interés del solicitante, esto es, que no están forzados a realizar estudios o investigaciones y mucho menos a someterla a un proceso de elaboración o de transformación.- - - - -

ANTECEDENTES:

1. Con base en los artículos 6 de la *Constitución Política de los Estados Unidos Mexicanos*; 4 bis de la *Constitución Política del Estado Libre y Soberano de Tabasco*; 3, fracciones VII, VIII y XV; 4, 6, 49, 50, fracciones III, VI, XI y XVII de la *Ley de Transparencia y Acceso a la Información Pública del Estado de*

² Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco.

"**Artículo 19.** Los Sujetos Obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones.

Artículo 20. Se presume que la información debe existir si se refiere a las facultades, competencias y funciones que los ordenamientos jurídicos aplicables otorgan a los Sujetos Obligados." (sic)



Tabasco; 15, fracciones III, XVI y XXII del *Reglamento Interior del Órgano Superior de Fiscalización del Estado* (vigente), la STYT tiene por recibida la solicitud de acceso a la información en comento.-

2. En ese contexto, se precisa que la fracción III del artículo 15 del citado Reglamento, prevé que la STYT se encarga de mantener una coordinación y comunicación permanente con las unidades administrativas de este Sujeto Obligado, relacionada con los asuntos que derivan del ejercicio de sus facultades, objetivos, acciones, metas o programas del ente obligado, por lo que, el Titular de la STYT al operar como un enlace directo con todas las áreas administrativas que integran al Órgano Superior de Fiscalización del Estado, puede pronunciarse respecto a la información solicitada conforme a las consideraciones siguientes:

- El artículo 19 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, señala que *"los Sujetos Obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones"*; es decir, que las solicitudes de acceso a la información necesariamente deben versar sobre documentos previamente generados o en posesión de los Sujetos Obligados, ya que el Derecho de Acceso a la Información tiene por objeto garantizar el acercamiento de la ciudadanía a la información pública contenida en los documentos que se encuentren en sus archivos, lo que implica la búsqueda de determinada información en el ente público de que se trate, NO encontrándose éste obligado a generar o elaborar documentos de acuerdo al interés del solicitante; es decir, que la obligatoriedad de proporcionar información por parte de una entidad gubernamental, no comprende el procesamiento de la misma, tal y como lo establece el último párrafo del numeral 6 de la Ley en la materia.- -----

De lo expuesto, y del conocimiento que se tiene de la información requerida, la STYT **ACUERDA**:

Primero. - La **DISPONIBILIDAD** de la información solicitada concerniente al *Documento de Seguridad de este Órgano Técnico*, por quien dijo llamarse **"ADAN AUGUSTO MAY RODRIGUEZ"**, en los términos siguientes:

- La STYT advierte que el pedimento informativo, va encaminado exclusivamente a la obtención de un documento en específico, referente al Documento de Seguridad del Órgano Superior de Fiscalización del Estado, siendo este 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 que posee"*³, el cual corresponde a un mandato dispuesto en los artículos 40 de la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco*; y 40 de los *Lineamientos de la*

³ Artículo 3, fracción XIII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco.



Ley de Protección de Datos Personales, concerniente a que cada "Responsable"⁴ de los Sujetos Obligados deberá elaborar dicho documento.- - - - -

- En ese tenor, por medio del presente se pone a disposición el Documento de Seguridad del Órgano Superior de Fiscalización del Estado vigente, debidamente integrado, conforme a los términos establecidos en la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco.- - - - -*

Segundo.- La **DISPONIBILIDAD** de la información peticionada, referente a los *Avisos de Privacidad que maneja el Órgano Superior de Fiscalización del Estado*, a través de la consulta de fuente pública, en los siguientes términos:

- La *Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Tabasco*, en la fracción I del artículo 3, establece que un "**Aviso de Privacidad**" es el 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.
- Al respecto, es de precisar que el Órgano Superior de Fiscalización del Estado, en cumplimiento a la normativa en la materia, cuenta con los Avisos de Privacidad de los Sistemas de Datos Personales vigentes, que este ente obligado emplea en el desempeño de sus funciones; a través de las diversas unidades administrativas que conforman la estructura orgánica de este Sujeto Obligado, mismos que se encuentran disponibles para su consulta a través de la página web oficial del OSFE, o ingresando directamente a liga electrónica siguiente:
http://www.osfetabasco.gob.mx/Objetos/Documentos/Aviso_Privacidad_OSF.html
- Cabe señalar que esta determinación, se realizó en apego a los términos del artículo 136 de la *Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco*, el cual señala:

"Artículo 136. Cuando la información requerida por el solicitante ya esté disponible al público en medios impresos, tales como libros, compendios, trípticos, registros públicos, en formatos electrónicos disponibles en Internet o en cualquier otro medio, se le hará saber por el medio requerido por el solicitante la fuente, el lugar y la forma en que puede consultar, reproducir o adquirir dicha información en un plazo no mayor a cinco días." (sic)

- Asimismo, es de precisar que la referida liga electrónica, en ningún momento transgrede el acceso a la información del solicitante; por lo tanto, se satisface la obligación de la STYT, contenida en la

⁴ En este caso, el Órgano Superior de Fiscalización del Estado, representado por el Fiscal Superior del Estado, de conformidad con la fracción XXVI del artículo 3 de la referida Ley.



hipótesis normativa del artículo 136, de la citada Ley de la materia, pues se trata de información que se encuentra disponible al público para su consulta en formatos electrónicos disponibles en internet, y solamente bastará hacerle del conocimiento al solicitante la fuente, el lugar y la forma en que puede consultar, reproducir o adquirir dicha información, tal y como aconteció en el presente asunto.

- Sirve de apoyo a lo anterior, el **Criterio 01/2005** emitido por el Comité de Acceso a la Información y de Protección de Datos Personales de la Suprema Corte de Justicia de la Nación, mismo que a continuación se transcribe:

"INFORMACIÓN DISPONIBLE EN MEDIOS IMPRESOS O ELECTRÓNICOS DE ACCESO PÚBLICO. PARA LA SATISFACCIÓN DEL DERECHO A SU ACCESO, BASTA CON FACILITAR AL SOLICITANTE SU CONSULTA, SIN QUE PARA SU CONOCIMIENTO SEA NECESARIA SU CERTIFICACIÓN. La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental tiene por objeto proveer lo necesario para que toda persona pueda tener acceso a la información pública gubernamental mediante procedimientos sencillos y expeditos. El espíritu de la Ley es privilegiar la agilidad del acceso a la información, razón por la cual el ejercicio de tal derecho respecto de aquella que se encuentre disponible en medios impresos o electrónicos de acceso público, se tiene por satisfecho al facilitar al solicitante su consulta, y su otorgamiento no implica la obligación del órgano de gobierno de certificar los datos en ella contenidos, máxime que ya se han hecho públicos. En efecto, el tercer párrafo del artículo 42 de la Ley invocada, considera que es suficiente que se haga saber al peticionario-por escrito-, la fuente, el lugar y la forma en que puede consultar, reproducir o adquirir la información disponible en medios impresos o electrónicos de acceso público; y el Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal para la aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en su artículo 22, segundo párrafo, precisa que se facilite al solicitante su consulta física y se le entregue, a la brevedad y en caso de requerirlo, copia de la misma. Por ello, para cumplir con el derecho de acceso a la información tratándose de este tipo de documentos, no es necesario ni debe requerirse de certificación, pues desde el momento en que el órgano de gobierno ha puesto a disposición del público tal información, ha asumido su autenticidad en contenido y forma. Además, cuando la normativa hace referencia a la modalidad de copia certificada, como una de las opciones para tener acceso a la información pública, debe entenderse que esta forma de acceder a la información es aplicable sólo en los casos en que aquélla no es consultable en una publicación oficial, lo que deriva de la propia ley, al disponer expresamente que para la satisfacción del derecho al acceso a la información gubernamental que se encuentra publicada en medios de acceso público, basta con facilitar su consulta."

Tercero.- La actuación de este Sujeto Obligado se desarrolló con apego al **Principio de Buena Fe**, entendido éste como un principio que obliga a todos a observar una determinada actitud de respeto, lealtad y honradez en el ámbito jurídico, tanto cuando se ejerza un derecho como cuando se cumpla un deber, y por ello este Órgano en uso de sus atribuciones, atendió la solicitud conforme a su literalidad; por lo que la presente determinación, satisface el **DAI** del particular.-----

Cuarto.- Hágase del conocimiento al particular, que en los términos de los artículos 148, 149 y 150 de la *Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco*, puede interponer Recurso



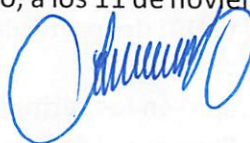
de Revisión si así lo considera, ante esta Unidad Administrativa o ante el Instituto Tabasqueño de Transparencia y Acceso a la Información Pública. -----

Quinto.- Notifíquese al solicitante el presente Acuerdo, y el **Documento de Seguridad de este Sujeto Obligado debidamente integrado y vigente**, a través del medio señalado en su pedimento identificado con el folio número **270509400008324**, de conformidad con el artículo 132 primer párrafo de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco; ahora bien, en cuanto a los anexos de dicho documento, será publicado en los Estrados Electrónicos de este Sujeto Obligado, ubicado en el Portal de Transparencia en la siguiente liga electrónica: http://www.osfetabasco.gob.mx/objetos/documentos/Cont_pot/estrados.html debiendo dar clic en el ícono de **"ESTRADOS ELECTRÓNICOS"** (sic), posteriormente seleccionará al apartado denominado **"Anexos"** (sic) y por último los rubros **"Anexo_1_Base_de_Datos"**, **"Anexo_2_Acuerdo_de_Responsabilidades"**, **"Anexo_3_Análisis_de_Riesgos"**, **"Anexo_4_Análisis_de_Brecha"** y **"Anexo_5_Bitácora"**; ello en virtud de que por el volumen de la información solicitada es imposible adjuntarlo en un solo archivo, ya que éste excede la capacidad permitida de 15 MB por la Plataforma Nacional de Transparencia. -----

Sirve de apoyo a lo anterior, el **Criterio 001/2015** emitido por el Instituto Tabasqueño de Transparencia y Acceso a la Información Pública, mismo que a continuación se transcribe:

"Portal de Transparencia. Permite la entrega electrónica de la información solicitada cuando supere la capacidad de envío permitida por el sistema de uso remoto Infomex-Tabasco. De conformidad con lo establecido en los artículos 8, 16 y 51 de la Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco; y 3 fracción VII y VIII de su Reglamento, la vía preferente para otorgar el acceso a la información pública es la electrónica y, la herramienta informática para la gestión remota de solicitudes de información es el Sistema Infomex-Tabasco. Igualmente, el Portal de Transparencia posee características similares a dicho sistema, como son: gratuidad, garantía de anonimato y seguridad jurídica; en ese sentido, para aquellos casos en que la respuesta a la solicitud supere la capacidad de envío por el sistema, resulta válido que se garantice el acceso a la misma, a través de su publicación en los estrados electrónicos de los Portales de Transparencia de los Sujetos Obligados."

Así lo acuerda, manda y firma, el **Lic. Jorge Alberto Franco Zurita**, Titular de la Secretaría Técnica y Transparencia del Órgano Superior de Fiscalización del Estado, ante la Lic. Wendoline Vera Mireles, Jefa del Departamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en la ciudad de Villahermosa, Tabasco, a los 11 de noviembre del año 2024.----- **Cúmplase.**



Elaboró: Lic. Wendoline Vera Mireles. Jefa del Departamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.



DOCUMENTO DE SEGURIDAD DE LOS SISTEMAS DE DATOS PERSONALES

ÓRGANO SUPERIOR DE FISCALIZACIÓN
DEL ESTADO



Contenido

1. Glosario
2. Introducción
3. Objetivo y Alcance
4. Inventario de Datos Personales y de los Sistemas de Tratamiento de los Datos
5. Funciones y Obligaciones de las personas que traten Datos Personales
6. Análisis de Riesgos
7. Análisis de Brecha
8. Plan de Trabajo
9. Mecanismos de Monitoreo y Revisión de las Medidas De Seguridad
10. Programa General de Capacitación

Anexos

Glosario.

Para los efectos del presente documento de seguridad, se entenderá por:

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.

Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionado a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

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

CTOSFE: Comité de Transparencia del Órgano Superior de Fiscalización del Estado.

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

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.

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 este. 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.

Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Días: Días hábiles.

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.

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.

Encargado: El servidor público o prestador de servicios contratado por honorarios, que realizará el tratamiento de datos personales a nombre y por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

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.

ITAIP: Instituto Tabasqueño de Transparencia y Acceso a la Información Pública (Órgano Garante).

LGTAIP: Ley General de Transparencia y Acceso a la Información Pública.

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

LLPDPPOET: Lineamientos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco.

LPDPPOET: Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco.

LTAIPET: Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco.

"2021. Año de la Independencia"

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.

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, y clasificación borrado seguro de la información, 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, mas no limitativa, se deben considerar las siguientes actividades:

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

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

- a) Prevenir que el acceso a las bases de datos o a la información, así como 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, 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.

OSFE: Órgano Superior de Fiscalización del Estado.

Plataforma nacional: Plataforma Nacional de Transparencia, la que hace referencia el artículo 49 de la LGTAIP.

"2021. Año de la Independencia"

Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano.

Responsable: Los sujetos obligados a que se refiere el párrafo tercero del artículo 1 de la LPDPPSOET, que deciden y determinan los fines, medios y demás cuestiones relacionadas con determinado tratamiento de datos personales.

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

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

STYT: Secretaría Técnica y Transparencia: Unidad a la que hace referencia el Capítulo IV, del Título Segundo, de la LTAIPET.

Supresión: La baja archivista 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.

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

Transferencia: Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas de manera enunciativa mas 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.

Unidad de Transparencia: Instancia a la que hace referencia el Capítulo IV, del Título Segundo, de la LTAIPET.

Introducción.

Los artículos 6, apartado A, fracción II y 16 de la *Constitución Política de los Estados Unidos Mexicanos*; 4 bis, fracción III de la *Constitución Política del Estado Libre y Soberano de Tabasco*, establecen como derecho fundamental la protección de datos personales¹ que tiene toda persona, los cuales deben ser protegidos conforme a los términos y excepciones que fijen las leyes en la materia.

Por su parte, los numerales 1, 2, 4, 6, 8, 43, 44, 45, 46 y 47 de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*; 1, 2, 4, 6, 8, 49, 50, 51, 52 y 53 de la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco*; 1, 3, 4, 57, 58, 59 y 60 de los *Lineamientos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco*, precisan un conjunto de bases, principios, procedimientos, funciones, obligaciones y condiciones para garantizar el derecho a la protección de datos personales y el ejercicio de los Derechos de Acceso, Rectificación, Cancelación, Oposición y de Portabilidad de los datos personales, que se encuentran en posesión de los sujetos obligados, dentro de los cuales se considera, conforme al artículo 1, tercer párrafo de la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco*, el Órgano Superior de Fiscalización del Estado.

Al respecto, en cumplimiento a lo establecido por la normativa aplicable en la materia, este sujeto obligado, como "responsable"² de los datos personales que posee, **emite el presente Documento de Seguridad**, el cual tiene sustento en los dispositivos 3, fracción XIII y 40 de la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco*; 40, 41, 42, 43, 44, 45, 46 y 47 de los *Lineamientos de la Ley* antes citada, mismo que se define como "*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.*"(sic)

Dicho documento de seguridad tiene como propósito establecer el marco normativo del tratamiento de los datos personales que se llevan a cabo al interior del Órgano Superior de Fiscalización del Estado, por las diversas unidades administrativas que conforman su

¹ Artículo 3, fracción VIII de la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco*:

"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;"

² *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco*:

"Artículo 3. Para los efectos de la presente Ley se entenderá por:

...

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;"

"2021. Año de la Independencia"

estructura orgánica, para efectos de mantener vigente y promover la mejora continua en la protección de datos personales, en términos de lo previsto en los artículos 40 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco; y 40 de los Lineamientos de la referida Ley.

En ese tenor, el Órgano Superior de Fiscalización del Estado, con base a los numerales 40, primer párrafo de la *Constitución Política del Estado Libre y Soberano de Tabasco*; 75 primer párrafo y 82 de la *Ley de Fiscalización Superior del Estado de Tabasco*; 8, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23 y 24 del *Reglamento Interior del Órgano Superior de Fiscalización del Estado*, ha identificado los procesos que en el ámbito de su competencia involucran el tratamiento de datos personales en **32 Sistemas de Datos Personales**³, a los cuales se les aplicarán las disposiciones del presente documento de seguridad, para efectos de mantener el resguardo y seguridad de los mismos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo a las respectivas funciones, ello conforme a los términos⁴ de los citados Lineamientos.

³ Numeral tres, fracción XIII de los Lineamientos para la Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco, (anteriores):

"XIII. Sistema de Datos Personales o Sistema. Conjunto organizado de datos personales que están en posesión de los Sujetos Obligados, y se encuentran contenidos en sus archivos, registros, ficheros, bancos o bases de datos, con independencia de su forma de creación, acceso, organización y almacenamiento;"

⁴ Artículo 40 de los Lineamientos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco.

Objetivo y Alcance

El Órgano Superior de Fiscalización del Estado, a través de su "**responsable**" tiene como objetivo garantizar la vigencia de los principios de protección de datos personales y de los derechos de los particulares personas en lo relativo a los tratamientos de datos personales llevados a cabo por el "**responsable**", con apoyo del "**encargado**" y "**sub encargados**" a través de los 32 Sistemas de Datos Personales que maneja este Órgano Técnico en el ejercicio de sus funciones y atribuciones, conforme lo dispuesto en el Título Cuarto de la *Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco*, así como, el Título Sexto de los *Lineamientos de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco*.

Lo anterior, mediante la precisión de las medidas de seguridad administrativas, físicas y técnicas que ha adoptado este ente público, para efectos de poder garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee, de igual forma, a través de la determinación de las posibles vulnerabilidades, amenazas y riesgos de los que puedan ser objeto dichos datos personales.

Inventario de datos personales y de los sistemas de tratamiento de los datos

De conformidad con los artículos 40, fracción I del de la LPDPPSOET, y 41 de los LLPDPPSOET, el **"responsable"** del OSFE deberá elaborar con base a sus Sistemas de Datos Personales, un *"inventario de datos personales y de los sistemas de tratamiento"* con el propósito de identificar, entre otros aspectos, la categoría y tipo de datos personales que son sometidos a tratamiento, incluyendo los de carácter sensible, los medios a través de los cuales se obtienen dichos datos, el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de los servidores públicos que tienen acceso al tratamiento, además de si son objeto de la transferencia y la identificación de los destinatarios o receptores de los mismos, así como las causas que la justifican.

Atento a lo anterior, en el OSFE se realizaron una serie de actividades con cada una de las unidades administrativas de este Órgano Técnico, para efectos de que de acuerdo a sus funciones, analizaran cada uno de sus procesos y tareas que involucran el tratamiento de datos personales, a fin de actualizar e integrar de manera adecuada su *"inventario de datos personales y de los sistemas de tratamiento"*.

Del resultado de dicha actividad, se reportaron operaciones y/o procedimientos de fiscalización, jurídicos, administrativos, de recursos humanos, materiales y financieros; de capacitaciones, y en materia de acceso a la información pública y protección de datos personales, reflejándose en un total **32** sistemas de datos personales, mismos que se describen a continuación:

Unidad Administrativa	Sistema de Datos Personales	
	No.	Denominación
Secretaría Particular (SP)	1	Control de Visitas
	2	CORRE
Unidad Técnica del Servicio Fiscalizador de Carrera (UTSFC)	3	Expedientes de los Integrantes del Servicio Fiscalizador de Carrera
	4	Registro a la Bolsa de Trabajo
	5	Convocatorias del Servicio Fiscalizador de Carrera
	6	Sistema de Registro y Control de Capacitaciones (SICAP)
	7	Cartera de Instructores

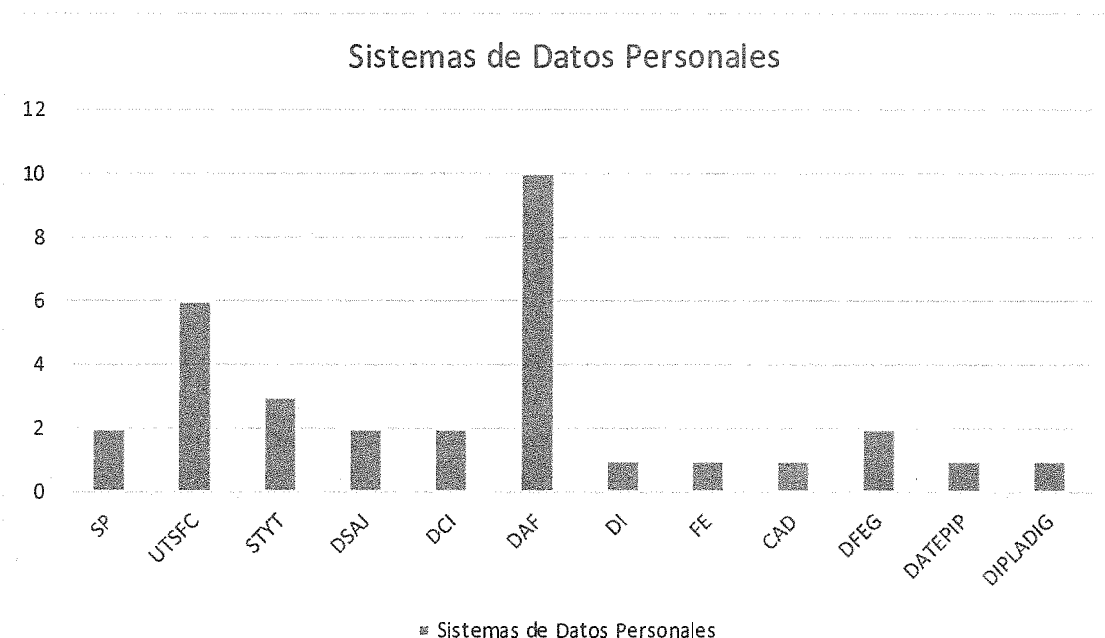
"2021. Año de la Independencia"

	8	Reclutamiento, Selección y Promoción de Fiscalización bajo el régimen de Honorarios
Secretaría Técnica y Transparencia (STYT)	9	Expedientes de Solicitudes de Acceso a la Información Pública y de Derechos ARCO
	10	Eventos Institucionales
	11	Difusión Institucional
Dirección de Substanciación y Asuntos Jurídicos (DSAJ)	12	Procedimientos para el Fincamiento de Responsabilidades Resarcitorias
	13	Procedimientos Administrativos de Multa
Dirección de Contraloría Interna (DCI)	14	Declaraciones Patrimoniales y de Intereses
	15	Integración de Expedientes para la Elaboración de Actas Circunstanciadas de Hechos
Dirección de Administración y Finanzas (DAF)	16	Padrón de Proveedores
	17	Plantilla y Expediente de Personal
	18	Control de Asistencia
	19	Plantilla y Expediente de Estudiantes que Prestan su Servicio Social y Práctica, Estadías o Residencias Profesional
	20	Nómina para el Pago de Salarios, Prestaciones y Honorarios
	21	Licencias de Conducir
	22	Adquisiciones
	23	Cuentas por Pagar
	24	Abastecimiento
	25	Siniestro de Vehículos Oficiales
Dirección de Investigación (DI)	26	Procedimientos de Investigación de Presuntas Responsabilidades Administrativas
Fiscalía Especial (FE)	27	Integración de los Informes de Resultados de la Revisión y Fiscalización de la Cuenta Pública
Coordinación de Auditoría del Desempeño (CAD)	28	Sistema de Datos de las Auditorías del Desempeño

"2021. Año de la Independencia"

Dirección de Fiscalización y Evaluación Gubernamental (DFEG)	29	Expedientes Técnicos de las Auditorías de Cumplimiento con Enfoque Financiero
	30	Sistema de Nombramientos y de Expedición de Constancias de Antigüedad Laboral de Servidores Públicos
Dirección de Auditoría Técnica y Evaluación a Proyectos de Inversión Pública (DATEPIP)	31	Evidencias del Proceso de Fiscalización de las Auditorías de Cumplimiento con Enfoque Técnico
Dirección de Planeación, Desarrollo Institucional y Gestión Documental (DIPLADIG)	32	Control de Registros de Servidores Públicos por Asesoría, Diplomados y/o Cursos Virtuales

De lo anterior se puede advertir que la unidad administrativa del OSFE con más número de sistemas en los que se tratan datos personales es la Dirección de Administración y Finanzas con un total de **10** sistemas, seguida por la Unidad Técnica del Servicio Fiscalizador de Carrera con **6**, la Secretaría Técnica y Transparencia con **3**, la Secretaría Particular, la Dirección de Substanciación y Asuntos Jurídicos, la Dirección de Contraloría Interna y la Dirección de Fiscalización y Evaluación Gubernamental con **2**; la Dirección de Investigación, la Fiscalía Especial, la Coordinación de Auditoría del Desempeño y la Dirección de Auditoría Técnica y Evaluación a Proyectos de Inversión Pública con **1** Sistema, tal y como se muestra a continuación:



Ahora bien, del análisis realizado a la "**BASE DE DATOS**" de cada uno de los 32 sistemas descritos, se advierte que las categorías a las que corresponden los datos personales tratados, son los siguientes:

- Identificables
- Biométricos
- Características Físicas
- Salud
- Informáticos
- Patrimoniales
- Laborales
- Académicos
- Procedimientos Seguidos en Forma de Juicio
- Naturaleza Pública

Cada unidad administrativa, reportó lo siguiente:

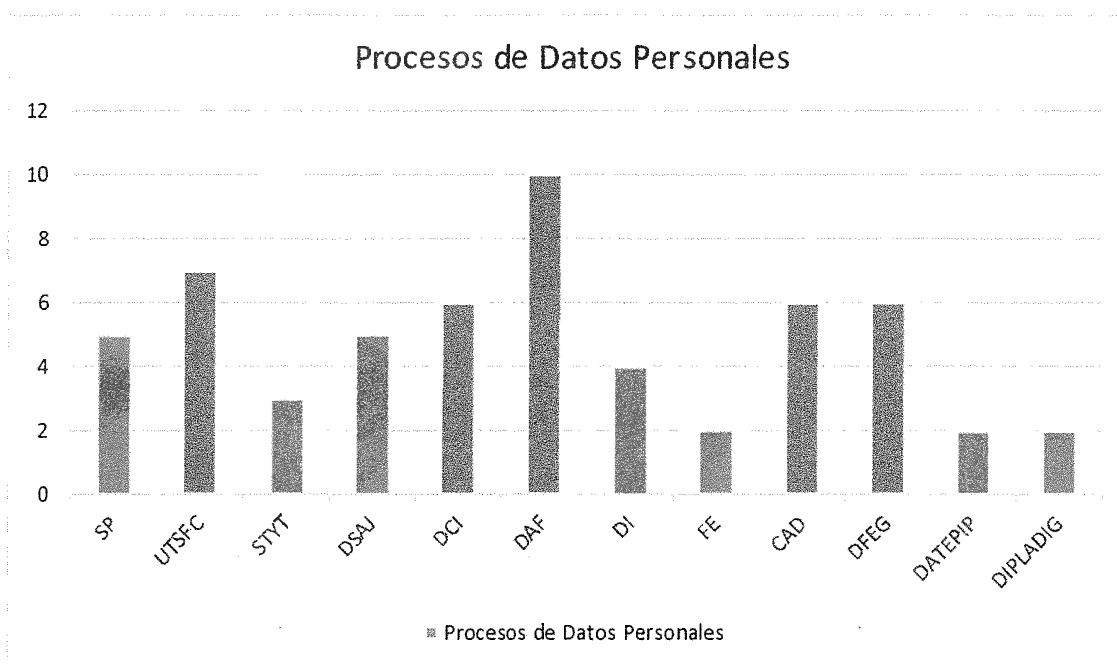
Unidad Administrativa	Categorías
Secretaría Particular	Identificables
	Informáticos
	Patrimoniales
	Laborales
	Académicos
Unidad Técnica del Servicio Fiscalizador de Carrera	Identificables
	Características Físicas
	Sensibles
	Informáticos
	Laborales
	Académicos
	Naturaleza Pública
Secretaría Técnica y Transparencia.	Identificables
	Informáticos
	Características Físicas
Dirección de Substanciación y Asuntos Jurídicos.	Identificables
	Informáticos
	Académicos

	Procedimientos Seguidos en Forma de Juicio
	Naturaleza Pública
Dirección de Contraloría Interna	Identificables
	Informáticos
	Patrimoniales
	Laborales
	Académicos
	Procedimientos Seguidos en Forma de Juicio
Dirección de Administración y Finanzas	Identificables
	Características Físicas
	Salud
	Informáticos
	Patrimoniales
	Laborales
	Académicos
	Procedimientos Seguidos en Forma de Juicio
	Naturaleza Pública
	Biométricos
Dirección de Investigación	Identificables
	Características Físicas
	Informáticos
	Especialmente Sensibles
Fiscalía Especial	Identificables.
	Procedimientos Seguidos en Forma de Juicio
Coordinación de Auditoría del Desempeño	Identificables
	Salud
	Informáticos
	Patrimoniales
	Laborales
	Naturaleza Pública
	Identificables

"2021. Año de la Independencia"

Dirección de Fiscalización y Evaluación Gubernamental	Biométricos
	Salud
	Informáticos
	Laborales
	Académicos
Dirección de Auditoría Técnica y Evaluación a Proyectos de Inversión Pública	Identificables
	Informáticos
Dirección de Planeación, Desarrollo Institucional y Gestión Documental	Identificables
	Informáticos

Lo anterior, permite determinar que la DAF es la unidad administrativa con más categorías de datos personales con **10**, seguida por la UTSFC con **7**, la DCI, la CAD y la DFEG con **6**; la SP y la DSAJ con **5**; la DI con **4**, la STYT con **3**, la FE, la DATEPIP y la DIPLADIG con **2** categorías, y como se visualiza a continuación:



De lo expuesto, se puede concluir que la categoría de datos personales con mayor número de áreas y procesos son los **IDENTIFICABLES**, seguidos por los Informáticos y, en casos muy específicos los de salud, biométricos y especialmente sensibles; sin embargo, es de señalar que se detectaron sistemas en los que se realiza tratamiento de datos personales de dos o

"2021. Año de la Independencia"

más categorías. Dicha información puede consultarse en el **Anexo 1** del presente documento de seguridad, consistente en las 32 **"BASE DE DATOS"** de los sistemas de datos personales del OSFE, requisitadas y firmadas por cada una de las unidades administrativas que realizan tratamiento de datos personales, conforme lo dispone el artículo 41 de los LLPDPPSOET.

Funciones y obligaciones de las personas que tratan datos personales

Los artículos 38, fracción II; 40, fracción II; 66, 67 y 68 de la LPDPPSOET, en relación con los numerales 40, fracción II; 42, 67 y 68 de los LLPDPPSOET, disponen que mediante contrato o cualquier otro instrumento jurídico, se deben establecer de manera clara y precisa las funciones y responsabilidades, así como el tratamiento que realizarán a los datos personales que manejan en sus sistemas de datos personales, el "**responsable**", "**encargados**" y "**sub encargados**" de los Sujetos Obligados.

En atención a lo anterior, y a raíz de los 32 sistemas de datos personales determinados en el inventario de datos personales del OSFE, este Órgano Técnico con base en las funciones y atribuciones de las unidades administrativas vinculadas con el tratamiento de datos personales, define tres roles básicos para el óptimo tratamiento de los mismos, siendo representados por los siguientes cargos:

Rol	Cargo del Servidor Público Designado
Responsable	Fiscal Superior del Estado
Encargado	Secretaria Particular
	Titular de la Unidad Técnica del Servicio Fiscalizador de Carrera
	Secretario Técnico
	Directora de Substanciación y Asuntos Jurídicos
	Directora de Contraloría Interna
	Directora de Administración y Finanzas
	Directora de Investigación
	Fiscal Espacial
	Coordinadora de Auditoría del Desempeño
	Director de Fiscalización y Evaluación Gubernamental

"2021. Año de la Independencia"

	Director de Auditoría Técnica y Evaluación a Proyectos de Inversión Pública
	Director de Planeación, Desarrollo Institucional y Gestión Documental
Sub encargado	Servidores Públicos designados por cada uno de los "Encargados", que en el ejercicio de sus funciones realicen tratamiento de Datos Personales.

Dichos roles se encuentran establecidos en los **"ACUERDOS DE RESPONSABILIDADES DE LOS ENCARGADOS DE LOS SISTEMAS DE DATOS PERSONALES"** que firmaron el **"responsable"** y el **"encargado(a)"** de cada uno de los 32 sistemas de datos personales del OSFE, consultables en el **Anexo 2** del presente documento; en los que, conforme a los numerales 66 de la Ley en la materia, y 42 de los Lineamientos citados, se describen las obligaciones y funciones de cada rol, mediante las siguientes cláusulas:

- **"PRIMERA. OBJETO DEL ACUERDO"**
- **"SEGUNDA. OBLIGATORIEDAD"**
- **"TERCERA. DISPOSICIONES GENERALES"**
- **"CUARTA. TRATAMIENTO DE DATOS"**
- **"QUINTA. ABSTENCIÓN DE TRATAMIENTO DISTINTO"**
- **"SEXTA. MEDIDAS DE SEGURIDAD"**
- **"SÉPTIMA. VULNERACIÓN DE DATOS"**
- **"OCTAVA. CONFIDENCIALIDAD"**
- **"NOVENA. DEVOLUCIÓN DE DATOS PERSONALES"**
- **"DÉCIMA. ABSTENCIÓN DE TRANSFERENCIA"**
- **"DÉCIMA PRIMERA. INSPECCIONES Y VERIFICACIONES"**
- **"DÉCIMA SEGUNDA. CONSERVACIÓN DE LA DOCUMENTACIÓN"**

Entre las obligaciones estipuladas en los instrumentos jurídicos citados, podemos observar las siguientes:

- Cumplimiento a cada una de las cláusulas del acuerdo
- Tratar únicamente los Datos Personales descritos en la **"BASE DE DATOS"** de cada Sistema de Datos Personales

“2021. Año de la Independencia”

- No realizar tratamiento distinto al especificado en los Sistemas de Datos Personales
- Aplicar las Medidas de Seguridad necesarias, para evitar vulneración de Datos Personales
- Informar inmediatamente al ***“responsable”*** alguna vulneración a las medidas de seguridad y a los Datos Personales
- Compromiso de guardar la confidencialidad de la información que contenga Datos Personales aun cuando la relación laboral haya terminado
- Devolver toda la información que Contenga Datos Personales, al momento de terminar la relación laboral
- Realizar solo las transferencias especificadas en la ***“BASE DE DATOS”*** de cada Sistema de Datos Personales
- El sub-Encargado se compromete a permitir que el ***“encargado(a)”*** y el ***“responsable”*** realicen inspecciones y verificaciones de los sistemas de Datos Personales que manejan
- El ***“encargado(a)”*** se compromete a generar, actualizar y conservar la documentación necesaria, con la finalidad de cumplir con las disposiciones normativas en la materia.

De lo expuesto, se advierte que todos los servidores públicos de este Órgano Técnico que tengan acceso a datos personales, están obligados a conocer y aplicar las medidas de seguridad propias de cada sistema en el que se concentren los datos, aplicable en todas y cada una de las fases del tratamiento de los datos personales, iniciando desde la obtención de los mismos y finalizando con su eliminación. Cabe mencionar que la obligación de confidencialidad, debe subsistir aún después de que los involucrados hayan finalizado su participación en el tratamiento de los datos personales porque hayan cambiado de funciones y aun cuando la relación laboral con la institución haya concluido, ya que en caso de incumplimiento al acuerdo y a las disposiciones normativas en la materia, se aplicará las sanciones estipuladas en las fracciones III, IV, VI, VII, IX y X del artículo 152 de la LPDPPSOET.

Análisis de riesgos

El artículo 43 de los LLPDPPSOET, dispone que el **"responsable"** de cada sujeto obligado debe elaborar un análisis de riesgos de los sistemas de datos personales que en el ejercicio de sus funciones implementa, el cual consiste en la identificación y evaluación del riesgo actual y real en el que se encuentren sus sistemas, así como las medidas para su reducción o mitigación.

En ese tenor, para la determinación del riesgo sobre la tipología de los datos personales que se manejan en dichos sistemas, se debe tomar en cuenta el tratamiento, el ciclo de vida de los datos personales, y la amenaza de la que pueden ser objeto. Aunado a lo anterior, con base en los **"ANÁLISIS DE RIESGOS"** de los 32 Sistemas de datos personales de este ente público, se consideran como riesgos, amenazas o vulneraciones, las siguientes:

Unidad Administrativa	Riesgos
Secretaría Particular	Sustracción de información del equipo de cómputo
	Contraseñas guardadas en la PC
	Robo del equipo de cómputo
	Sustracción de información física del archivo de trámite
	Extravío de información durante el proceso de remisión
	Compartir usuarios y contraseñas entre el personal autorizado y no autorizado
	Sustracción de la información electrónica a través de Sistema, por falta de control de registro del historial de descarga de archivos por parte de los usuarios autorizados
Unidad Técnica del Servicio Fiscalizador de Carrera	Sustracción de los expedientes de la oficina de la UTSFC
	Incendio de la oficina

"2021. Año de la Independencia"

	Ataque cibernético
	Daño en el servidor informático
	Extravío de expediente físico
	Sustracción de los expedientes físicos del proceso
	Sustracción de los expedientes electrónicos del proceso
	Hackeo del Sistema
Secretaría Técnica y Transparencia	Extraviar un expediente
	Sustracción de un expediente de la oficina
	Sustracción de un expediente del equipo de cómputo
Dirección de Substanciación y Asuntos Jurídicos	Extraviar un expediente
	Sustracción de Archivos Electrónicos
	Sustracción de Archivos Físicos
Dirección de Contraloría Interna	Personal adscrito al Departamento de Recursos Humanos capture datos erróneos del Servidor Público
	El Sistema DECLAR@OSFE permita el ingreso de externos que puedan visualizar, descargar e imprimir información de los servidores públicos registrada en el sistema
	Los Encargados con acceso al SDP, hagan mal uso de la información presentada por los servidores públicos
	Integración y Clasificación incorrecta de los expedientes
	Que personal ajeno al Departamento tenga acceso a

	los expedientes y obtengan información de los mismos
	Extraviar un expediente
Dirección de Administración y Finanzas	Sustracción de expediente archivero y/o oficina
	Sustracción de información digital
	Divulgación o uso indebido de datos sensibles
	Manipulación de información por personas no autorizadas
	Extravío de expediente
	Sustracción de la información biométrica o de huella dactilar del personal
	Divulgación de la información confidencial que contiene la nómina
Dirección de Investigación	Perdida de los archivos
	Sustracción de un expediente
	Sustracción de un expediente del equipo de cómputo
Fiscalía Especial	Extravío de un Informe de Resultados impreso
	Sustracción de un Informe de Resultados de la oficina
	Sustracción de un Informe de Resultados de los equipos de cómputo
Coordinación de Auditoría del Desempeño	Extravío o robo de un expediente, o información física o digital
	Sustracción de un expediente físico o electrónico
	Robo de computadora e comisión

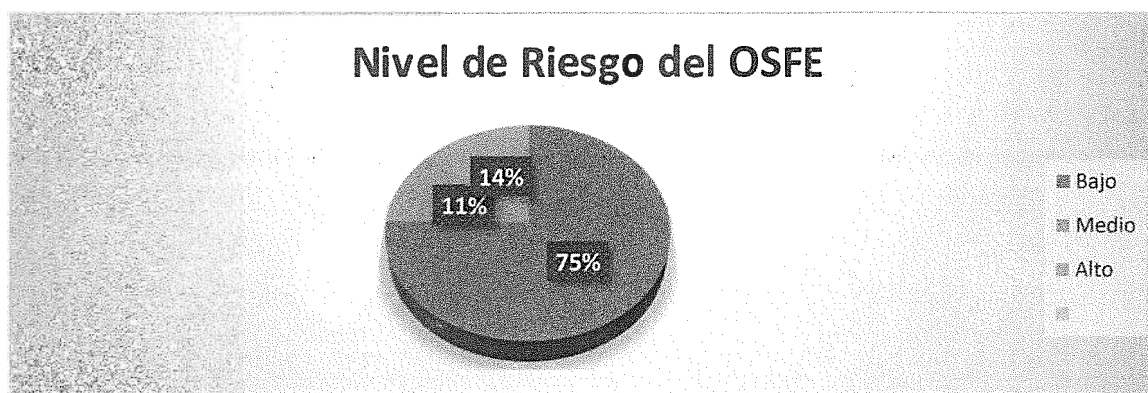
"2021. Año de la Independencia"

Dirección de Fiscalización y Evaluación Gubernamental	Sustracción de expedientes o archivos electrónicos
	Robo de los equipos de cómputo
	Extravío de documentos
Dirección de Auditoría Técnica y Evaluación a Proyectos de Inversión Pública	Extravío de un expediente
	Substracción de un expediente de la oficina
Dirección de Planeación, Desarrollo Institucional y Gestión Documental	Pérdida del expediente
	Extracción indebida del expediente
	Sustracción de archivos electrónicos de los equipos de cómputo

Entre las más comunes tenemos:

- Extravío de Expediente Físico.
- Sustracción de Expediente Físico o Electrónico.
- Robo de equipo de cómputo.
- Uso, acceso o tratamiento no autorizado.
- Otras.

De los riesgos descritos en la relación anterior, se tomó en cuenta la *"Evaluación"* o *"Nivel de Riesgo"* bajo, medio o alto de que la amenaza suceda en los sistemas de datos personales del OSFE; por lo que, con base en dichos formatos, se tiene que las unidades administrativas que tratan datos personales, en total identificaron **73** niveles de riesgos, de los cuales **55** son bajo, **8** corresponde a medio y **10** a alto. En ese tenor, se determina que el *"Nivel de Riesgo"* que predomina en este Órgano Técnico es el **BAJO**, tal y como se muestra a continuación:



"2021. Año de la Independencia"

Dicha información puede consultarse en el **Anexo 3** de este documento, consistente en los 32 **"ANÁLISIS DE RIESGOS"** de los Sistemas de Datos Personales del OSFE, requisitados y firmados por cada una de las unidades administrativas que realizan tratamiento de datos personales, conforme lo dispone el artículo 43 de los LLPDPPSOET.

Análisis de brecha

Una vez identificados los posibles riesgos a los que este sujeto obligado se encuentra susceptible de enfrentar, podemos realizar el "**ANÁLISIS DE BRECHA**", que dispone el numeral 44 de los referidos Lineamientos, del cual se advierte que el "**responsable**" de cada sujeto obligado deberá identificar y evaluar las medidas de seguridad que implementa en sus sistemas de datos personales, con las medidas de seguridad faltantes y de ser el caso, la creación de nuevas medidas que pudieran ayudar a remplazar uno o más controles implementados actualmente.

Al respecto, es de señalar que las medidas de seguridad **administrativas** son el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; **físicas**, corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, **técnicas**, que se valen de la tecnología para proteger el entorno digital de la información.

En ese tenor, y con base en lo expuesto en el punto que antecede, cada "**encargado(a)**" y "**sub encargado(a)**" mediante una encuesta, determinaron de manera detallada las medidas de seguridad administrativas, físicas y técnicas con las que cuentan sus sistemas de datos personales, así como las faltantes y la nuevas medidas que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados, para efectos de mitigar los riesgos a los que están expuestos los datos personales tratados, concluyendo que actualmente este sujeto obligado tiene un nivel de medidas de seguridad óptimo en relación con los datos personales que manejan en sus sistemas de datos personales. Información consultable en el **Anexo 4** del presente documento.

Plan de trabajo

La Secretaría Técnica y Transparencia del Órgano Superior de Fiscalización del Estado, elabora el presente Plan de Trabajo en materia de datos personales en el OSFE, conforme a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco, y lo pone a disposición de cada uno de los servidores públicos que laboran en este Órgano Técnico, y en especial a los que funjan como **"encargados"** y **"sub encargados"** de los sistemas de datos personales para efectos de cumplir y garantizar la protección de los datos personales que se encuentran en su posesión, el cual detalla las actividades que deberá realizar este sujeto obligado para la constante actualización de los 32 sistemas de datos personales de este ente público. Lo anterior, en razón de que conforme a los artículos 89, fracción V y 90, fracciones III y VII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco; y 15, fracción XV del Reglamento Interior del Órgano Superior de Fiscalización del Estado, el Comité de Transparencia y la Secretaría Técnica y Transparencia tienen como función el garantizar la vigencia de los principios de protección de datos personales y de los derechos de las personas en lo relativo a los tratamientos de datos personales llevados a cabo por el **"responsable"**, **"encargado"**, y en su caso **"sub encargado"**, tal y como lo establece el Título Cuarto de la LPDPPSOET, así como el Título Sexto de los LLPDPPSOET.

La Protección de Datos Personales corresponde a la garantía de tutela de la privacidad de datos personales en poder de los sujetos obligados; es decir, es un derecho fundamental de las personas físicas que busca proteger su intimidad y su privacidad frente a las vulneraciones de tales derechos que puedan proceder de la obtención y almacenamiento de sus datos personales por las diferentes unidades administrativas que conforman la estructura orgánica del Órgano Superior de Fiscalización del Estado.

Este derecho se encuentra fundamentado en:

Cuerpo Normativo.	Transcripción.	Interpretación.
Artículo 6, apartado A, fracción II de la Constitución Política de los Estados Unidos Mexicanos.	<i>"II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes."</i>	Los numerales descritos refieren a la información confidencial (Datos Personales), que no tiene el carácter de información pública y solo es accesible para su titular o su representante legal, misma que deberá ser protegida en los términos y con las excepciones que fijen las leyes aplicables. Además, que
Artículo 16, párrafos primero y segundo de la Constitución Política de los Estados Unidos Mexicanos.	<i>"Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud</i>	

	<p><i>de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.</i></p> <p><i>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."</i></p>	<p><i>si bien, NO está sujeta al Principio de Máxima Publicidad; también lo es que la normativa en la materia precisa circunstancias excepcionales en las que la protección a la vida privada o los datos personales pueden subordinarse al interés público.</i></p> <p>Esta determinación se hace mediante un procedimiento que se conoce como la <i>Prueba de Interés Público</i>, concerniente a la ponderación de los intereses para determinar que cierta información perteneciente al ámbito privado puede ser divulgada porque existe una razón de interés público que así lo justifica.</p>
<p>Artículo 4 bis, fracción III de la Constitución Política del Estado Libre y Soberano de Tabasco.</p>	<p><i>"III. El derecho a la intimidad que incluye la privacidad de la vida familiar en primer grado y en general la que se refiere a sus datos personales, deberá ser garantizado por el Estado</i></p>	<p>Considerado también como un derecho fundamental que protege el derecho a la intimidad y a la privacidad de la vida familiar y respecto de sus Datos Personales el cual debe ser garantizado por el Estado en los términos y</p>

"2021. Año de la Independencia"

	<i>en los términos y excepciones que fijen las leyes, teniendo siempre como referente el respeto a la dignidad humana;"</i>	excepciones que fijen las Leyes.
Artículo 1 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Tabasco	<i>"Artículo 1. La presente Ley es de orden público y de observancia general en todo el Estado de Tabasco, en los términos previstos por el artículo 4º BIS de la Constitución Política Local; y por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus Datos Personales, en posesión de sujetos obligados en el orden estatal y municipal."</i>	Dicha ley tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la Protección de sus Datos Personales.
Lineamientos de la ley de protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Tabasco.	<i>"Artículo 1. Los presentes Lineamientos tienen por objeto desarrollar las disposiciones previstas en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco."</i>	Este documento normativo tiene como objetivo el regular el manejo de los tratamientos de los Sistemas de Datos Personales que conforme al desempeño de sus funciones y atribuciones emplea este Órgano Técnico.

De lo anterior, es de señalar que son datos de carácter personal todos aquellos que se refieren a una persona física identificada o identificable, desde su nombre hasta cualquier otro dato que revele información sobre sus hábitos, preferencias, formas de vida, etc.

Al respecto, el artículo 3, fracción VIII de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco, define a los **Datos Personales** como *"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"* (sic). Es cualquier 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.

En virtud de lo expuesto, es dable precisar que la protección de datos personales que resguarde y posea este sujeto obligado, así como sus tratamientos, serán a cargo del Órgano Superior de Fiscalización del Estado (OSFE Tabasco) en su calidad de **"responsable"**, tal y como lo establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Tabasco en su artículo 3, fracción XXVI que a la letra señala:

"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;"

Los dispositivos 19 y 20 de los Lineamientos de la citada Ley, refieren que el **"responsable"**, en este caso el OSFE, en apego a la normativa aplicable implementará capacitaciones, políticas y programas de protección de datos personales que tengan u obtengan en el ejercicio de sus funciones, mismos que deberán ser aprobados, coordinados y supervisados por su Comité de Transparencia.

Por lo que, para efectos de cumplir con lo anterior, el Sujeto Obligado debe contar con **"encargados"** y **"sub encargados"** de los sistemas de datos personales que manejen; por lo que, la Secretaría Técnica y Transparencia deberá coordinar de manera **semestral** (en junio y diciembre de cada año) las actualizaciones de dichos sistemas y del documento de seguridad, mediante las **actividades** siguientes:

Actualización de la información de los sistemas de datos personales que implementan las unidades administrativas.

- Se requerirá a los titulares de las áreas administrativas que conforman la estructura orgánica del OSFE Tabasco, para efectos de que en su rol de **"encargado(a)"** **comuniquen** a la Secretaría Técnica y Transparencia, la implementación de algún sistema de datos personales o en su caso, la baja de alguno de los reportados en su última actualización, o bien, si no ha ocurrido cambio o modificación de los mismos.

"2021. Año de la Independencia"

Asimismo, se solicitará se **designe al o los sub encargados (as)** por cada uno de los sistemas reportados, debiendo proporcionar los siguientes datos: unidad administrativa, nombre del enlace, categoría, correo electrónico y extensión telefónica.

Requisición de las "BASES DE DATOS" de los sistemas de datos personales.

- Se **remitirá** a los enlaces de transparencia de cada una de las unidades administrativas que hayan reportado sistemas de datos personales, el formato denominado **"BASE DE DATOS"** en el cual deberán detallar por sistema, la información solicitada en el mismo.
- Se citará a las unidades administrativas a reunión de trabajo, para despejar cualquier duda.
- El documento requisitado deberá **presentarse** ante la Secretaría Técnica y Transparencia, de manera física y electrónica, debidamente firmado.

Elaboración de los avisos de privacidad simplificados e integrales de los sistemas de datos personales.

- Se **requerirá** a los titulares de las unidades administrativas, para efectos de que elaboren por cada sistema de datos personales un aviso de privacidad simplificado y uno integral, toda vez que se tiene el imperativo de mantener informado al titular de los datos personales que se recaben en el ejercicio de atribuciones, sobre los alcances, tratamiento y finalidad con la que se solicitan.
- Se citará a las unidades administrativas a reunión de trabajo, para despejar cualquier duda.
- El documento requisitado deberá **presentarse** ante la Secretaría Técnica y Transparencia, de manera física y electrónica.

Suscripción del "ACUERDO DE RESPONSABILIDADES DE LOS ENCARGADOS DE LOS SISTEMAS DE DATOS PERSONALES".

- Se **remitirá** a los titulares de las unidades administrativas, el formato del acuerdo citado, para efectos de que por sistema de datos personales lo requisen, para que posteriormente lo **presenten** a la Secretaría referida, debidamente firmados para que se turne a firma del **"responsable"** del OSFE.
- Se citará a las unidades administrativas a reunión de trabajo, para despejar cualquier duda.
- El documento requisitado deberá **presentarse** ante la Secretaría Técnica y Transparencia, de manera física y electrónica.

"2021. Año de la Independencia"

Requisición de los "ANÁLISIS DE RIESGO" y "ANÁLISIS DE BRECHA" de los sistemas de datos personales.

- Se **remitirá** a los enlaces de transparencia de cada una de las unidades administrativas que hayan reportado sistemas de datos personales, los formatos denominados **"ANÁLISIS DE RIESGOS"** y **"ANÁLISIS DE BRECHA"** en los cuales deberán detallar por sistema, la información solicitada en el mismo.
- Se citará a las unidades administrativas a reunión de trabajo, para despejar cualquier duda.
- Los documentos requisitados deberán presentarse ante la Secretaría Técnica y Transparencia, de manera física y electrónica.

Publicación y actualización de los avisos de privacidad.

- Una vez que se haya concluido cada una de las actividades descritas, y con apoyo en la Dirección de Tecnologías de la Información se solicitará actualización de los avisos de privacidad en el sitio web oficial de este Órgano Técnico.
- Asimismo, cada titular de las áreas administrativas instruirá a su personal la colocación del aviso de privacidad simplificado de cada uno de sus sistemas de datos personales, en las instalaciones de sus oficinas.

Actualización final, aprobación y publicación del Documento de Seguridad del OSFE.

- Por último, en el mes de diciembre de cada año, mediante sesión ordinaria se le presentará a los integrantes del Comité de Transparencia, el Documento de Seguridad de este Órgano Técnico, para efectos de que analicen y aprueben dicho Documento.
- Posteriormente, y con apoyo de la Dirección de Tecnologías de la Información se publicará en la página oficial web de este Órgano Técnico el Documento de Seguridad citado.

Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad

Los numerales 3, fracción XX; 36, 38, fracción VII; 40, fracción VI; 89, fracción VI de la LPDPPSOET, y 46 de los LLPDPPSOET, disponen que el Comité de Transparencia de los sujetos obligados será la autoridad máxima en materia de protección de datos personales, en la organización del **"responsable"**, por lo que deberá supervisar en coordinación con las unidades administrativas que realicen tratamiento de datos personales, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad.

En ese tenor, el Comité de Transparencia del OSFE deberá realizar de manera **semestral** (junio y diciembre) los monitoreos y evaluaciones de las medidas de seguridad administrativas, físicas y técnicas que cada una de las unidades administrativas reportaron en sus **"ANÁLISIS DE BRECHA"** de los 32 sistemas de datos personales que maneja este Órgano Técnico en el ejercicio de sus funciones, lo anterior para efectos de vigilar el cumplimiento de la normativa aplicable en la materia, así como las disposiciones de este documento de seguridad, a través de los siguientes mecanismos:

Mecanismo	Objetivo
Realizar visitas a las unidades administrativas (3).	Verificar de primera mano la aplicación, actualización e impacto de las medidas de seguridad aplicadas.
Solicitar reportes a los responsables de cada área generadora de información, o a los responsables del sistema de datos personales o a sus administradores, sobre el manejo de datos personales conforme a las medidas de seguridad.	Monitorear avances, aplicación, eventualidades y novedades respecto a la aplicación de las medidas de seguridad.

Es de precisar que este ente público, para reforzar el resguardo de los documentos, expedientes, archivos, etc. tanto físicos como electrónicos, cuenta con mecanismos de oficialías de parte y caseta de vigilancia, los cuales restringen el acceso a las instalaciones a personas ajenas o no autorizadas en esta institución; esto con la finalidad de tener mejores controles de seguridad y eliminar el riesgo de que se pueda sustraer, extraviar o alterar los documentos, expedientes o archivos resguardados.

Ahora bien, en caso de ocurrir alguna vulneración a las medidas de seguridad implementadas por este sujeto obligado, o a los datos personales que se traten en los sistemas de datos personales, los artículos 43, 44 y 45 de la LPDPPSOET; y 49 y 50 de los Lineamientos de la referida Ley, establecen que el **"responsable"** deberá llevar un registro

“2021. Año de la Independencia”

de las mismas, a través de una ***“bitácora de vulneraciones de seguridad”*** en la cual se precisará los siguientes elementos:

- Hora y fecha en que sucedió la vulneración
- Descripción detallada de las circunstancias en torno a la vulneración ocurrida
- Descripción de las posibles consecuencias de la vulneración de seguridad ocurrida
- Cualquier otra información y documentación que considere conveniente hacer de conocimiento al Órgano Garante y al Titular de los Datos Personales
- Categoría de los Datos Personales y el número de Titulares afectados
- Sistemas de Datos Personales comprometidos

Es de señalar que en el caso práctico de este ente público dicha bitácora estará a cargo de cada uno de los ***“encargados”*** de los sistemas de datos personales reportados, con la finalidad de llevar un mejor control de los mismos, y así poder notificar al ***“responsable”*** la vulneración dentro de las 24 horas, tal y como lo señala el formato denominado ***“bitácora de vulneraciones de seguridad”***, consultable en el **Anexo 5** del presente documento.

Posteriormente, el ***“responsable”***, de conformidad con los artículos 44 y 45 de la LPDPPSOET, notificará dichas vulneraciones al titular y al Órgano Garante dentro de las 72 horas en cuanto se confirmen.

En virtud de lo expuesto, se determina que la supervisión de las medidas de seguridad que implementa este Órgano Técnico en sus 32 sistemas de datos personales, son primordiales para valorar las amenazas, vulnerabilidades, aplicación correcta o incorrecta, impacto y actualización de las mismas, esto con el objetivo de que las medidas de seguridad aplicadas por el OSFE continúen siendo las efectivas e idóneas, para la mejora continua en materia de protección de datos personales.

Programa General de Capacitación.

El OSFE, conforme a lo establecido en los artículos 38, fracción VIII, 40 fracción VII de la LPDPPSOET, y 47 de los LLPDPPSOET, que plantean que el responsable deberá diseñar e implementar programas que tengan por objeto capacitar a los servidores públicos considerando sus facultades y responsabilidades asignadas para el tratamiento de y seguridad de los datos personales que traten con motivo de sus funciones y atribuciones,

Con motivo de la actualización semestrales de los sistemas de datos personales, este Órgano Técnico realizará de manera semestral las diferentes capacitaciones en materia de protección de datos personales, así como también gestionará la impartición de capacitaciones por parte de Instituto Tabasqueño de Transparencia y Acceso a la Información Pública (ITAIP), a todo el personal involucrado con el tratamiento de datos personales de este ente fiscalizador.

Cabe resaltar que uno de los factores esenciales para la implementación de controles y demás medidas de seguridad, así como la actualización y mejora continua del inventario de datos personales, el apego a la normatividad, así como la concientización en la materia por parte del personal involucrado en el tratamiento de datos personales, es el conocimiento y capacitación, por lo que el aprovechamiento de los recursos y herramientas que el propio OSFE ha dispuesto para su uso y obtención de beneficios, se propone que a través de la Secretaría Técnica y Transparencia con apoyo del Comité de Transparencia, se desarrolle un programa de capacitación focalizada, mediante el cual profundice en el conocimiento de la materia por parte de los servidores públicos que intervienen en el tratamiento de datos personales.

Así entre los temas de mayor relevancia que resultan necesarios profundizar y capacitar al personal del OSFE, se encuentran los siguientes:

- | | |
|--|-------------------------------------|
| I.- Sensibilización respecto a la protección de datos personales | III.- Base de datos |
| I.- Protección de Datos Personales | IV.- Inventario de datos personales |
| II.- Marco normativo | V.- Documento de seguridad |
| | VI.- Avisos de Privacidad |

Es de precisar que las fechas exactas de las capacitaciones que impartirá la Secretaría Técnica y Transparencia de este Órgano Técnico, se notificará a los titulares de cada una de las unidades administrativas, al menos con una semana de anticipación a la fecha de la capacitación, para efectos de que comuniquen y asignen a su personal que asistirá.

ANEXOS

