DOCUMENTO DE SEGURIDAD DE LA

PROMOTORA PARA LA CONSERVACIÓN Y DESARROLLO SUSTENTABLE DEL ESTADO DE CAMPECHE.

Índice.

I. INTRODUCCIÓN.

En el presente documento se detallan las medidas de seguridad de la Promotora para la Conservación y Desarrollo Sustentable del Estado de Campeche para garantizar la debida protección de los datos personales a los que se les da tratamiento en las direccionesque los manejan.

Con este documento de seguridad se da cumplimiento al artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados publicado el día 26 de enero de 2017, el cual a la letra dice:
De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

i. El inventario de datos personales y de los sistemas de tratamiento;
ii. Las funciones y obligaciones de las personas que traten datos personales;
iii. El análisis de riesgos;
iv. El análisis de brecha;
v. El plan de trabajo;
vi. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y
vii. El programa general de capacitación.

II. GLOSARIO DE TÉRMINOS.

Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;

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;

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;

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad puedadeterminarse directa o indirectamente a través de cualquier información;

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;

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

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;

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 yrevisión 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, enmateria de protección de datos personales;

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

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

- Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización,recursos e información;
- Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que puedasalir de la organización, y
- Proveer a los equipos que contienen o almacenan datos personales de un mantenimientoeficaz, que asegure su disponibilidad e integridad;

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

- Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, seapor usuarios identificados y autorizados;
- Generar un esquema de privilegios para que el usuario lleve a cabo las actividades querequiere con motivo de sus funciones;
- Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimientodel software y hardware, y
- Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursosinformáticos en el tratamiento de datos personales;

Responsable: Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales

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

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

A continuación se describen las categorías de datos personales con los quecuenta la Promotora para la Conservación y Desarrollo Sustentable del Estado de Campeche, esto según el formato que se llenó por cada área.

- **Datos de identificación y contacto:** nombre, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales.
- **Datos laborales:** puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección y contratación y experiencia/capacitación laboral.
- **Datos académicos:** trayectoria educativa, título, cédula profesional, certificados y reconocimientos.
- **Datos patrimoniales y/o financieros:** ingresos y egresos.
- **Datos sobre pasatiempos, entretenimiento y diversión:** pasatiempos, aficiones, deportes que practica y juegos de interés.
- **Datos legales:** situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)
- **Datos de salud:** estado de salud físico presente.
- **Datos personales de naturaleza pública:** Datos que por mandato legalson de acceso público.

Personas de quienes se obtienen los datos personales:

a) Personas que laboran en La Promotora.

b) Personas externas que prestan algún servicio para La Promotora.

c) Personas externas que participan en actividades educativas, culturales y deportivas que se llevan a cabo en La Promotora.

Los datos personales se recaban por medio de documentos presentados y/o por el llenado de formularios físicos y/o electrónicos por los titulares de los datos personales.

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

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 la Ley.

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

Las áreas encargadas de tratar los datos personales son las siguientes:

a. Dirección General.
b. Coordinación Administrativa.
c. Unidad de Transparencia.
d. Unidad de Asuntos Jurídicos.
e. Secretaría Técnica

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

- Garantizar la seguridad en el tratamiento de datos personales, esto con la finalidad de evitar algún riesgo, como la pérdida, robo, alteración o acceso no autorizado.
- Garantizar la debida protección de los datos personales, conforme a la Ley ylas demás disposiciones aplicables en la materia.
- Implementar medidas de seguridad físicas, técnicas y administrativas convenientes para el tratamiento diario de los datos personales.
- Garantizar la confidencialidad de los datos personales derivada de losprocedimientos que tienen a su cargo.
- Conocer y aplicar las acciones derivadas de este Documento de Seguridad.
- Garantizar el cumplimiento de los derechos ARCO a los titulares de los datospersonales

V. 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 Áreas de la Promotora 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.

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

VI. IDENTIFICACIÓN Y AUTENTIFICACIÓN.

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.

VII. CONTROL DE ACCESO Y GESTIÓN DE SOPORTE.

En todo momento, las Áreas que dan tratamiento a datos personalesdeberán 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.

VIII. COPIAS DE RESPALDO Y RECUPERACIÓN.

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 Copias de respaldo y recuperación.

IX. ANÁLISIS DE RIESGOS.

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

- Robo, extravío o copia no autorizada.
- Destrucción no autorizada
- Daños por situaciones fortuitas

X. ANÁLISIS DE BRECHAS.

Derivado del estudio del cuestionario denominado “Medidas de seguridad existentesVS medidas de seguridad faltantes” el cual se aplicóa las Áreas se concluyó que, actualmente, se tiene un nivel de medidas de seguridad óptimo en relación con los datos personales que se manejan.

Asimismo, con las medidas de seguridad que se señalan en este documento de seguridad se pretende que queden asentadas y uniformes.

XI. EL PLAN DE TRABAJO.

El plan de trabajo para la protección de los datos personales que se llevará a cabo será cumplir con el proyecto que se tiene implementado por La Promotora, el cual se denomina “Certificación a Sujetos Obligados en materia de Datos Personales”, que cuenta con los siguientes pasos:

- Canalizar a cada unidad administrativa que trate datos personales, la encuesta sobre el estado actual del cumplimiento de las obligaciones en materia de datos personales para que sea contestada y así poder conocer las áreas de oportunidad con las cuales se trabajará.
- Capacitar al personal en materia de datos personales e informarlesdel proyecto de Certificación.

- Implementar medidas de seguridad físicas, administrativas y técnicas para la debida protección de los datos personales.
- Conformar el documento de seguridad como lo requiere la Ley.
- Llevar a cabo visitas de seguimiento y de verificación, esto con el objetivo de corroborar el cumplimiento de las obligaciones que marca la Ley.
- Conformar la carpeta de evidencia del cumplimiento de las obligaciones según la para que ésta sea revisada y aprobada.
- De ser aprobada la carpeta de evidencia, el ICAI tendrá por cumplidas las obligaciones de la Ley.

XII. 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, esto de acuerdo a sus funciones y obligaciones.

XIII. LOS PROGRAMAS DE CAPACITACIÓN Y ACTUALIZACIÓN.

El personal sé capacitará en materia de protección de datos personales una vez al año, la fecha se designará en el transcurso del mismo, esto con la intención de que todos estén presentes.

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.

XIV. ACTUALIZACIÓN DEL DOCUMENTO DE SEGURIDAD.

El presente documento de seguridad se actualizará cuando ocurran los siguienteseventos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personalesque deriven en un cambio en el nivel de riesgo;
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- Como resultado de un proceso de mejora para mitigar el impacto de unavulneración a la seguridad, e
- Implementación de acciones correctivas y preventivas ante una vulneraciónde seguridad.
- Cuando surjan documentos, formatos, recomendaciones, etc. por parte del INAI para la mejora del documento de seguridad.

XV. ANEXOS.

Anexo1

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

Anexo2

ANÁLISIS DE RIESGO Amenazas, vulnerabilidades y recursos involucrados				
Código	**Pregunta o Control**	**¿Existe? SI**	**¿Existe?NO**	**Observaciones (acciones a realizar en caso de no contar con:**
1.- Amenazas				
1.1	*¿Tienes identificado los datos personales?*			
1.2	*¿Tienes clasificados los datos personales?*			
1.3	*¿Tienes establecido el ciclo de vida de los datospersonales?*			
1.4	*¿Tienes definido el tratamiento que se le da a cada uno de los datos personales?*			
1.5	*¿Tienes capacitaciones sobre qué hacer en caso de que los datos personales queden expuestos?*			
1.6	*¿Tienes un catalogo sobre las consecuencias negativas para los titulares de los datos personales?*			
1.7	*¿Tienes un plan reactivoen caso de sufrir la pérdida de datos personales?*			
1.8	*¿Tienes una bitácora de las causas que originaron el daño al sistema y por ende a los datos personales?*			
1.9	*¿Tienes registro de las amenazas surgidasdurante la implementación, puesta en marcha y desarrollo*			

	del sistema, el cual contiene datos personales?			
1.10	*¿Tienes contemplado el riego inherente al tipo de dato personal vulnerado?*			
1.11	*¿Tienes contemplado elriego por el volumen de titulares afectados?*			
2. vulneraciones				
2.1	*¿Tienes una bitácora sobre vulneraciones sufridas en los datospersonales?*			
2.2	*¿Tienes requerimientos regulatorios en caso de vulneración de los datos personales?*			
2.3	*¿Tienes una política a seguir en caso de daño al sistema por una vulneración de los datos personales?*			
2.4	*¿Tienes códigos de conducta del personal que trata datospersonales?*			
2.5	*¿Tienes claro elbeneficio para el atacante al obtener los datos personales?*			
2.6	*¿Tienes un sistema de todas y cada unas de las consecuencias que surgieron a raíz de la vulneración del sistema que contiene datos personales?*			
2.7	*¿Tienes procedimientos para actuar ante la vulneración de los sistemas de datos personales?*			
3. recursos involucrados				
3.1	*¿Tienes un software para descubrir la anonimidad del atacante de los datos personales?*			
3.2	*¿Tienes respaldos en el caso de que la información fue vulnerada?*			
3.3	*¿Tienes hardware y software para respaldarlos datos personales?*			
3.4	*¿Tienes personal capacitado para llevar a*			

	cabo los respaldos hardware y software que contendrán los datos personales?			
3.5	*¿Tienes calendario, con fechas para dar servicio y mantenimiento a los sistemas, computadoras, discos duros, hardware ysoftware en los que se almacenan datos personales?*			
3.6	*¿Tienes asesoría externa para dar servicio y mantenimiento a los sistemas, computadoras, discos duros, hardware ysoftware en los que se almacenan datos personales?*			

Anexo 3

ANÁLISIS DE BRECHA Medidas de seguridad existentes y medidas de seguridad faltantes				
Código	Pregunta o Control	¿Existe? SI	¿Existe? NO	Observaciones
1.- Medidas de seguridad basadas en la cultura del personal				
1.1	*¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?*			
1.1.1	Política de escritorio limpio			
1.1.2	Hábitos de cierre y resguardo			
1.1.3	Impresoras, escáneres, copiadoras y buzones limpios			
1.1.4	Gestión de bitácoras, usuarios y acceso			
2.-	*¿Tienes mecanismos para eliminar de manera segura la información?*			
2.1	Destrucción segura de documentos			
2.2	Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico			
2.3	Fijar periodos de retención y destrucción de información			
2.4	Tomar precauciones con los procedimientos de re-utilización			

2.5	*¿Has establecido y documentado los compromisos respecto a la protección de datos?*			
3.- Medidas de seguridad basadas en la cultura del personal				
3.1	Informar al personal sobre sus deberes mínimos de seguridad y protección de datos			
3.2	Fomentar la cultura de la seguridad de la información			
3.3	Difundir noticias en temas de seguridad			
3.4	Prevenir al personal sobre la *Ingeniería Social*			
3.5	Asegurar la protección de datos personales en subcontrataciones			
4	*¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?*			
4.1	Tener un procedimiento de notificación.			
4.2	Realizar revisiones y auditorías.			
5	*¿Realizas respaldos periódicos de los datos personales?*			
6.- Medidas de seguridad en el entorno de trabajo físico				
6.1	*¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?*			
6.1.1	Alerta del entorno de trabajo.			
6.1.2	Mantener registros del personal con acceso al entorno de trabajo			
6.2.1	*¿Tienes medidas de seguridad para evitar el robo?*			
6.2.2	Cerraduras y candados			
6.2.3	Elementos disuasorios.			
6.2.4	Minimizar el riesgo oportunista.			
6.3	*¿Cuidas el movimiento de información en entornos de trabajo físicos?*			
6.3.1	Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico			

6.3.2	Mantener en movimiento sólo copias de la información, no el elemento original			
6.3.3	Usar mensajería certificada			
7.- Medidas de seguridad en el entorno de trabajo digital				
7.1	*¿Realizas actualizaciones al equipo de cómputo?*			
7.2	*¿Revisas periódicamente el software instalado en el equipo de cómputo?*			
7.3	*¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?*			
7.3.1	Uso de contraseñas y/o cifrado			
7.3.2	Uso de contraseñas solidas			
7.3.3	Bloqueo y cierre de sesiones			
7.3.4	Administrar usuarios y accesos			
7.4	*¿Revisas la configuración de seguridad del equipo de cómputo?*			
7.5	*¿Tienes medidas de seguridad para navegar en entornos digitales?*			
7.5.1	Instalar herramientas antimalware y de filtrado de tráfico			
7.5.2	Reglas de navegación segura			
7.5.3	Reglas para la divulgación de información			
7.5.4	Uso de conexiones seguras			
7.6	*¿Cuidas el movimiento de información en entornos de trabajo digitales?*			
7.6.1	Validación del destinatario de una comunicación			
7.6.2	Seguridad de la información enviada y recibida			

INVENTARIO DE DATOS PERSONALES.

Marcar con una **X** los datos personales que existen y son necesarios o que existen más no sonnecesarios en los procesos administrativos de su Área.

Datos personales recabados.	Existente.	Necesario.	No necesario.
Datos de identificación y contacto.			
Nombre:			
Estado Civil:			
Registro Federal de Contribuyentes (RFC):			
Clave Única de Registrode Población (CURP):			
Lugar de nacimiento:			
Fecha de nacimiento:			
Nacionalidad:			
Domicilio:			
Teléfono particular:			
Teléfono celular:			
Correo electrónico:			
Firma autógrafa:			
Firma electrónica:			
Edad:			
Fotografías			
Referencias personales:			

Datos sobre características físicas.			
Color de piel:			
Color de cabello:			
Señas particulares:			
Estatura:			
Peso:			
Cicatrices:			
Tipo de sangre:			
Datos biométricos.			
Imagen del iris:			
Huella dactilar:			
Palma de la mano:			
Datos laborales.			
Puesto o cargo que desempeña:			
Domicilio de trabajo:			
Correo electrónico institucional:			
Teléfono institucional:			
Referencias laborales:			
Información generada durante los procedimientos de reclutamiento, selecciónу contratación:			
Experiencia/Capacitación laboral:			

Datos académicos			
Trayectoria educativa:			
Títulos:			
Cédula profesional:			
Certificados:			
Reconocimientos:			
Datos migratorios.			
Entrada al país:			
Salida del país:			
Tiempo de permanenciaen el país:			
Calidad migratoria:			
Derechos de residencia:			
Aseguramiento:			
Repatriación.			

Datos patrimoniales y/o financieros.			
Bienes muebles:			
Bienes inmuebles:			
Información fiscal:			
Historial crediticio/Buróde crédito:			
Ingresos:			
Egresos:			
Cuentas bancarias:			
Números de tarjetas de crédito:			
Información adicional de tarjeta (fecha de vencimiento, códigos deseguridad, datos de banda magnética, pin):			
Seguros:			
Afores:			

Datos sobre pasatiempos, entretenimiento y diversión.			
Pasatiempos:			
Aficiones:			
Deportes que practica:			
Juegos de su interés:			
Datos legales.			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros):			
Otros datos personales (mencionar).			
Datos personales recabados:	**Existente.**	**Necesario.**	**No necesario.**

Datos personales recabados.	Existente.	Necesario.	No necesario.
Datos personales sensibles.			
Datos sobre la ideología.			
Posturas religiosas/ ideológicas/morales/ filosóficas:			
Pertenencia a un partido/Posturas políticas:			
Pertenencia a un sindicato:			
Datos de salud.			
Estado de salud físico presente, pasado o futuro:			
Estado de salud mental presente, pasado o futuro:			
Información genética:			
Datos sobre vida sexual			
Preferencias sexuales:			
Prácticas o hábitos sexuales:			
Datos de origen étnico o racial.			
Pertenencia a un pueblo,etnia o región:			
Otros datos personales (mencionar).			