DOCUMENTO DE SEGURIDAD

EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES
EN POSESIÓN DE LA COORDINACIÓN DE
COMUNICACIÓN SOCIAL DEL
GOBIERNO DEL ESTADO DE SINALOA.

I. Introducción.

El derecho de acceso y rectificación de los datos personales en el Estado de Sinaloa encuentra su antecedente en la Ley de Acceso a la Información Pública del Estado de Sinaloa, publicada en el año 2002.

El 20 de Julio de 2007, se reforma el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, en la cual se reconoce el derecho de acceso a la información como una garantía fundamental, las fracciones II y III tienen la virtud de ser las primeras menciones constitucionales expresas que hacen un reconocimiento del derecho a la protección de datos personales y se constituyen como limitantes al ejercicio del derecho de acceso a la información.

El 2009 se distingue por, la concreción de dos relevantes acontecimientos relacionados con la consolidación del derecho a la protección de datos en México, la aprobación de las reformas a los artículos 16 y 73 de la Constitución.

El artículo 16 constitucional incorpora a la lista de garantías fundamentales consagradas en nuestra Carta Magna, el derecho a la protección de datos personales y lo dota de contenido, a saber: *"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".*

Por su parte, el artículo 73 constitucional dota de facultades al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares.

El 13 de abril de 2010, la Cámara de Diputados aprobó el proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, por su parte, la Cámara de Senadores aprobó por unanimidad dicho dictamen, el 27 de abril de 2010 y finalmente, el 5 de julio de 2010 el Poder Ejecutivo Federal publicó en el Diario Oficial de la Federación la Ley.

El 26 de Julio de 2017 se publica la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa (LPDPPSOES), la cual entró en vigor al día siguiente de su publicación.

El 15 de Marzo de 2019, la Comisión Estatal para Acceso a la Información Pública, publicó el acuerdo mediante el cual se aprueba los Lineamientos de Protección de Datos Personales para Sujetos Obligados del Estado de Sinaloa.

A partir de la publicación de la LPDPPSOES y los Lineamientos de Protección de Datos Personales para Sujetos Obligados del Estado de Sinaloa, la Coordinación de Comunicación

Social del Gobierno del Estado de Sinaloa (CCS) adquiere el carácter de "Responsable'' y deberá tratar dichos datos conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; adoptar medidas de seguridad para la protección de los mismos; plasmar un documento de seguridad de dichas medidas, garantizar los derechos de acceso, rectificación , cancelación y oposición.

Entre los "deberes'' previstos en la LPDPPSOES, la CCS deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad, para lo cual la Unidad de Transparencia elaboró este documento.

II. Marco Normativo.
Para efectos de este documento, la normatividad aplicable es la siguiente:

- Artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos.
- Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).
- Ley General de Protección de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).
- Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa (LTAIPES).
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa (LPDPPSOES).
- Reglamento Interior de la Coordinación de Comunicación Social.
- Lineamientos de Protección de Datos Personales para Sujetos Obligados del Estado de Sinaloa.

III. Ámbito de aplicación.
En atención a los "deberes" que refiere la LPDPSOES, el presente documento es aplicable para todas las áreas de la CCS, que en el ejercicio de sus atribuciones y funciones, administren bases de datos en sistemas de tratamiento de datos personales, que tengan acceso a soportes físicos y/o electrónicos, con independencia de la forma o modalidad de su creación, procesamiento, almacenamiento y organización. Los datos personales podrán ser expresados en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o cualquier formato que haga identificable a una persona.

IV. Política de Protección de Datos Personales de la CCS.
La CCS protegerá los datos personales proporcionados a ésta, en base a lo dispuesto en la LPDPPSOES y los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa.

Objeto.
La Política de Protección de Datos Personales explica cómo se tratan y protegen los Datos Personales que sean recolectados por esta Coordinación, en todas sus bases de datos y/o archivos que contengan Datos Personales.

A. Responsable del Tratamiento de los Datos Personales y Fundamento para ello.
Conforme lo dispuesto en la LTAIPES y en la LPDPPSOES, la CCS es la responsable del tratamiento de los datos personales que le proporcionen, y el fundamento para tratar sus datos personales, se encuentra en los artículos 21 , 94, 165 y el segundo párrafo del artículo 166 de la LTAIPES y en los artículos 1, 2, 3, 4 fracción II, 14, 28, 29, 30, 31 , 32, 33, 34, 35, 36, 37 , 38, 196 fracción VIII de la LPDPPSOES.

B. Datos Sometidos a Tratamiento.
Los datos personales serán utilizados con la finalidad de:

a) Fomentar una participación más activa de los medios de información y los profesionales de la comunicación en la difusión de las actividades que realiza el Gobierno del Estado.
b) Mantener constantes relaciones con los representantes de los diversos medios masivos de comunicación y auxiliares para la realización de la cobertura informativa generada por el Estado.
c) Orientar a los titulares en el uso y manejo del presupuesto correspondiente y en los trámites ante la Secretaría de Administración y Finanzas.
d) Otorgr licencias y estímulos procedentes; atender todo lo relativo al pago de nóminas de las áreas adscritas a la coordinación.
e) Llevar y remitir a la Subsecretaría de Asuntos Jurídicos de la Secretaría General de Gobierno, los datos y la firma autógrafa de los servidores públicos adscritos.
f) Formular estudios con proyecciones presupuestales y programáticos tendientes a la mejora de calidad de los servicios que prestan las áreas adscritas.
g) Elaborar su programa de trabajo, formular y mantener actualizado sus manuales de organización y procedimientos, y a poyar a las unidades administrativas.
h) elaboración de sus respectivos presupuestos; atender todo lo relativo a los asuntos administrativos de las diferentes unidades administrativas.

Para las finalidades antes señaladas y dependiendo de los datos personales a tratar, se recaban los siguientes datos:

1) Nombre completo.
2) Estado civíl.
3) Edad.

4) Domicilio.
5) Nacionalidad.
6) Número telefónico.
7) Registro Federal de Contribuyentes.
8) Número de IMSS.
9) Correo electrónico.

C. Derechos de los Titulares de los Datos Personales.
Para el ejercicio de cualquiera de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) se deberá presentar la solicitud respectiva en la Unidad de Transparencia, con domicilio en Avenida Insurgentes s/n segundo piso, Colonia, Centro Sinaloa Culiacán, Sinaloa, C.P. 80129

Para conocer el procedimiento y requisitos para el ejercicio de los derechos ARCO se podrá llamar al siguiente número telefónico (667)758-70-00 Extensión 1362 para ponerse en contacto con nuestro Responsable de la Unidad de Transparencia, quien dará trámite a las solicitudes para el ejercicio de estos derechos y atenderá cualquier duda que se pudiera tener respecto al tratamiento de la información.

D. Área responsable de la implementación y observancia de esta política.
El Comité de Transparencia, a través de la Unidad de Transparencia, tiene a su cargo la labor de desarrollo, implementación, capacitación y observancia de ésta Política. Para tal efecto, todos los servidores públicos que realizan el *Tratamiento de Datos Personales* en las diferentes áreas de la CCS están obligados a reportar estas Bases de Datos y a dar traslado a ésta de manera inmediata de todas las peticiones, quejas o reclamos que reciban por parte de los Titulares de Datos Personales.

El Comité de Transparencia será responsable de la atención de peticiones, consultas, quejas y reclamos ante la cual el titular de la información podrá ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.

E. Autorización - Consentimiento.
El responsable deberá contar con el consentimiento previo del Titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:

- **I. Libre:** Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;
- **II. Específica:** Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento; e
- **III. Informada:** Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento al que serán sometidos sus datos personales.

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

El consentimiento podrá manifestarse de forma expresa o tácita:

- **Consentimiento expreso:** Es cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.
- **Consentimiento tácito:** Es cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del Titular se manifieste expresamente.

Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del Titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos de excepción previstos en el artículo 22 de la LPDPPSOES.

Se considerará que el consentimiento expreso se otorgó por escrito cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable. En el entorno digital podrán utilizarse medios como la firma electrónica o cualquier mecanismo o procedimiento equivalente que permita identificar fehacientemente al titular, y a su vez recabar su consentimiento de tal manera que se acredite la obtención del mismo.

El responsable deberá informar al Titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

F. Seguridad de los Datos Personales.

La CCS, en estricta aplicación del *Principio de Seguridad en el Tratamiento de Datos Personales,* proporcionará las medidas técnicas, físicas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su alteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. La obligación y responsabilidad de la CCS, se limita a disponer de los medios adecuados para este fin.

La CCS no garantiza la seguridad total de su información ni se responsabiliza por cualquier consecuencia derivada de casos fortuitos, causas de fuerza mayor, fallas técnicas o del ingreso indebido por parte de terceros a la Base de Datos o Archivo en los que reposan los Datos Personales objeto de Tratamiento por parte de la CCS.

G. Tratamiento de Datos Personales.
La CCS deberá darles un tratamiento a los datos personales recabados en estricto apego a los principios de Calidad, Confidencialidad, Consentimiento, Finalidad, Información, Lealtad y Legalidad en materia de tratamiento de datos personales, Licitud, Proporcionalidad, Responsabilidad y Seguridad, expresados en el Artículo 12 de la LPDPPSOES.

Se precisa que el servidor público que incumpla a los principios citados anteriormente será causa de sanción de acuerdo a lo dispuesto en el Artículo 196 de LPDPPSOES.

H. Vigencia.
Esta Política de Protección de Datos Personales está vigente desde la fecha de su aprobación por el Comité de Transparencia de la CCS.

V. Funciones y Obligaciones del personal involucrado en el tratamiento de datos personales.

Todos los servidores públicos que tengan acceso a los datos personales, están obligados a conocer y aplicar las medidas de seguridad propias que sean de carácter administrativo, físico y técnico para la protección de datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción, o en su caso, se deberá de garantizar la confidencialidad, integridad y disponibilidad.

Funciones genéricas en cualquier nivel de tratamiento:

- Tratar los datos personales con responsabilidad y las medidas de seguridad que se haya establecido para tal fin.

Obligaciones genéricas en cualquier nivel de tratamiento:

- Guardar confidencialidad sobre la información que se conozca en el desarrollo de sus actividades.
- Estar capacitado en materia de tratamiento de datos personales.
- Dar aviso a los superiores jerárquicos, ante cualquier acción que pueda poner en riesgo los datos personales, y en general que puedan vulnerar la seguridad de los datos personales.

El incumplimiento a lo establecido en este Documento de Seguridad, así como lo establecido por la LPDPPSOES, será causa de aplicación de medidas de apremio y/o sanción de acuerdo a lo dispuesto en el artículo 196 de LPDPPSOES.

VI. Inventarios de Datos Personales y de los Sistemas de Tratamiento

Los sistemas que se detallan en el presente documento son aquellos que contienen datos personales, que se encuentran tanto en soporte electrónico como físico.
Se presentan por Dirección y en orden con base al Reglamento Interior de la CCS.

A. Dirección de Relaciones Públicas

En los siguientes apartados, se estará abordando cada uno de los sistemas, señalando su descripción, estructura y medidas de seguridad. Dentro de este último se realizará un análisis de riesgos, el análisis de brecha y el plan de trabajo.

En la descripción de cada sistema de tratamiento de datos personales, se señala el fundamento legal; los datos personales que se encuentran en la dirección, la forma de obtención de los datos personales, el servidor público administrador del sistema, tipo de soporte, características del lugar físico donde se resguardan los datos personales, portabilidad de datos, transferencia de datos, encargado de datos.

Dirección de Relaciones Públicas

1.- Fundamento Legal.- Sección II Artículo 14 del Reglamento Interior de la Coordinación de Comunicación Social.

2.-Datos Personales que se encuentran en esta Unidad Administrativa:

INVENTARIO DE DATOS PERSONALES GENERALES
DIRECCION DE RELACIONES PÚBLICAS

Marque con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos o trámites llevados a cabo en su Unidad Administrativa.

Datos Personales Recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X		
Alias			
Seudónimo			
Sexo			
Estado Civil	X		
Registro Federal de Contribuyentes (RFC)	X		
Registro Federal del instituto Nacional (INE)			
Clave Unica de Registro de Población (CURP)			
Lugar de Nacimiento			
Fecha de Nacimiento			
Nacionalidad			
Domicilio	X		
Teléfono particular	X		
Teléfono celular personal	X		
Correo electrónico personal	X		
Firma autógrafa			
Firma electrónica			
Edad			
Fotografía			
Referencias personales			
Escolaridad			
Número de seguridad social o análogo			
Datos sobre características físicas			
Color de piel			
Color de cabello			
Señas particulares			
Estatura			
Peso			
Cicatrices			
Tipo de sangre			
Datos biomédicos			

1

3.- Forma de obtención de los datos personales. - Se obtienen mediante el registro de los mismos durante reuniones de trabajo, vía correo electrónico o llamadas telefónicas.

4.- Servidor Público Administrador de la Dirección:
Cargo: Jefe del Depto. de Recursos Humanos.
Teléfono y Extensión: (667)758-7000 ext. 1357
Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Reglamento Interior de la CCS, y realizar aquellas que le encomienden sus superiores jerárquicos.
Principales obligaciones: Mantener constantes relaciones públicas del Ejecutivo Estatal, con los representantes de los medios de comunicación social en el estado, promover una participación más activa en las actividades que realiza el Gobierno del Estado.

5.- Tipo de Soporte.- El soporte de los datos personales se encuentra en físico.

6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales.- Esta Unidad Administrativa se encuentra en Ave. Insurgentes s/n, segundo piso, Centro Sinaloa, Culiacán, Sinaloa. Los archivos físicos se encuentran en una oficina bajo llave, dentro de esta oficina están depositados en archiveros con llave.

7.- Portabilidad de datos.- Esta Unidad Administrativa no cuenta con ningún formato estructurado para la portabilidad de datos.

8.- Transferencia de datos.- Esta Unidad Administrativa no transfiere datos personales.

9.- Encargado de datos.- La Dirección de Relaciones Públicas.

VII. Medidas de Seguridad.
La LPDPPSOES, establece que se entenderá como medidas de seguridad al conjunto de acciones, actividades, controles o mecanismos administrativos, físicos y técnicos que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;

II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;

III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;

IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;

V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales; y

VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.

Derivado de lo anterior, el documento de seguridad debe contener al menos, el inventario de datos personales y de los sistemas de tratamiento, las funciones y obligaciones de las personas que traten datos personales, el análisis de riesgo, el análisis de brecha, el plan de trabajo, los mecanismos de monitoreo y revisión de las medidas de seguridad y el programa general de capacitación.

Las medidas de seguridad se abordaran en tres modalidades: administrativas, físicas y técnicas.

Las medidas de seguridad administrativas se traducen en políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Las medidas de seguridad físicas son el conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento.

Las medidas de seguridad técnicas son el 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.

Como medidas de seguridad, de manera general en la CCS, se cuenta con las siguientes:

De tipo físico:

a) Prevenir el acceso no autorizado al perímetro de la CCS, sus instalaciones físicas, áreas críticas, recursos e información.

Para lo anterior, la CCS se encuentra dentro de las instalaciones de la Unidad Administrativa del Gobierno del Estado de Sinaloa, el cual cuenta con personal de vigilancia que tiene por objeto la vigilancia, protección a instalaciones, bienes y personas en las oficinas que ocupa la CCS y el resto de las dependencias ahí ubicadas.

Tiene capacidad de respuesta inmediata y se ejecutan medidas de prevención, contención, neutralización y mitigación de los efectos adversos en el interior y la periferia de las oficinas, es decir, resguardan las instalaciones físicas, áreas críticas, recursos e información las 24 horas, los 365 días del año.

b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la CCS, recursos e información;

Se cuenta con normas, procedimientos y medidas de seguridad con el propósito de reducir al mínimo la incidencia de riesgos como: protocolo de acceso a las áreas estratégicas, protocolo ante sabotaje, protocolo por manifestaciones, protocolos de amenaza de bomba, protocolo de sismos y protocolo de incendios.

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización; y

En la CCS se cuenta con acciones y mecanismos que permiten proteger e identificar los equipos móviles y portátiles; mobiliario, documentos y materiales mediante controles de acceso al edificio tanto de entrada y salida, como son: control en el uso de aparatos electrónicos y eléctricos, control en el ingreso y egreso de aparatos, equipos, mobiliario, documentos y materiales previa autorización del Director de Área.

d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Los equipos de cómputo de escritorio y portátiles que la CCS asigna a los servidores públicos y áreas administrativas correspondientes para el cumplimiento de sus funciones, así como los equipos destinados al procesamiento, almacenamiento, transmisión y respaldo de la información relacionada a los Sistemas de Información, cuentan con mantenimiento periódico en el que se ejecutan acciones preventivas y en su caso, correctivas respaldadas por el personal de soporte técnico, con lo que se promueve un mantenimiento eficaz, disponibilidad de equipos y la información que hospedan.

De Tipo Técnico:
Se consideran aquellas medidas de seguridad aplicables en los sistemas de tratamiento de datos en soporte electrónico.

a) Prevenir que el acceso a las bases de datos personales o a la información, así como a los recursos, sea por usuarios identificados y autorizados;

El acceso a la base de datos es exclusivo para el personal responsable del tratamiento de los datos personales de cada área. El acceso a las bases de datos se efectúa a través de Usuarios y Contraseñas asignado a cada operador de su equipo de cómputo.

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

Las funciones del usuario de los sistemas de información, instituciones y de los responsables del tratamiento de datos personales en cada área, son definidas por las áreas responsables de los procesos respectivos.

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

La seguridad de todos los equipos de cómputo y de la red interna de Gobierno, está a cargo del personal de soporte técnico que cuenta con las herramientas tecnológicas para dicho fin como son firewalls, antivirus, servicio de internet corporativo y restringido para los usuarios.

d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

VIII. Análisis de Riesgos.
En el establecimiento de las medidas de seguridad, se deben considerar los riesgos existentes y la posibilidad de mitigarlos a través de un análisis cualitativo, sobre el impacto y la probabilidad de que se vulnere la seguridad, tanto en la información de datos

personales como en los recursos involucrados. Este apartado se desarrolló tomando en cuenta:

1) Los requerimientos regulatorios, mejores prácticas de un sector específico.
2) El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.
3) El valor y exposición de los activos involucrados en el tratamiento de los datos personales.
4) Las consecuencias negativas que para los titulares pudieran derivar de una vulneración de seguridad.
5) La sensibilidad de los datos personales tratados.
6) El desarrollo tecnológico.
7) Las posibles consecuencias de una vulneración para los titulares.
8) El número de titulares.
9) Las vulneraciones previas ocurridas.

Los factores pueden ser:	
Personas	Servidor público que se encuentra relacionado con el tratamiento y seguridad de los datos.
Procesos	Actividades y tareas necesarias para llevar acabo el tratamiento de los datos.
Tecnología	Conjunto de Herramientas tecnológicas que intervienen de manera directa o indirecta en tratamiento y seguridad de los datos.
Infraestructura	Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el sistema de datos.

La clasificación puede ser:	
TIC	Tecnologías de la información y comunicación. (Software y Hardware)
Capacitación	Capacitación Desconocimiento de los Procesos.
Control	Control Falta de control.
Recursos	Recursos Humanos, financieros, rnateriales.

El control puede ser:	
Interno	Si depende de la Dirección.
Externo	SI dependen de alguna otra Dirección.
Terceros	Si se refiere a algún ente externo a la SE.

Los valores pueden ser:		Valor	Semáforo	Nota
Impacto Alto =3	P. de O. Alto=3	9	Rojo	En caso de datos personales sensibles, el impacto siempre será alto.
	P. de O. Media=2	8	Rojo	
	P. de O. Bajo=1	7	Rojo	
Impacto Medio =2	P. de O. Alto=3	6	Naranja	
	P. de O. Media=2	5	Naranja	
	P. de O. Bajo=1	4	Naranja	
Impacto Bajo =1	P. de O. Alto=3	3	Amarillo	
	P. de O. Media=2	2	Amarillo	
	P. de O. Bajo=1	1	Amarillo	

IX. Análisis de Brecha.

En este apartado se consideraron las medidas de seguridad existentes y los riesgos identificados para determinar cuáles son las medidas de seguridad faltantes.

X. Plan de Trabajo.

Una vez realizado el análisis de riesgo y el análisis de brecha, cada unidad administrativa responsable de la protección de los datos personales elaboró un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para su cumplimiento cotidiano de la política y tratamiento de los datos personales.

XI. Metodología para la redacción y vinculación de la información.

Para el desarrollo de las medidas de seguridad actuales, el análisis de riesgo, el análisis de brecha y el plan de trabajo, se manejan claves de identificación (ID) como una herramienta metodológica para realizar referencias y evitar la repetición en la escritura, ya que todos los subtemas están vinculados.

Los ID a utilizar en el documento de seguridad están integrados por 4 dígitos alfanuméricos:
Primer digito: Empieza con una letra Mayúscula que corresponde a una Dirección de la CCS.
Segundo digito: Continúa con un número consecutivo del sistema de tratamiento de datos personales.
Tercer digito: Se incorpora un número consecutivo, seguido de un punto, según el tema que se trate. Así, cuando se refieren las medidas de seguridad, se utiliza el número 1, para los riegos o amenazas, se utiliza el número 2, al describir las brechas se utiliza el número 3 y la referencia del plan de trabajo, se hace con el número 4.
Cuarto digito: Finalmente se integra por otro número consecutivo, del 1 al "X", que indica el número de la medida, el riesgo, la brecha o la actividad referida.

Tipo	Control / Mecanismo	ID	Medidas actuales
Administrativas	Políticas interna de protección de datos personales	B1.1.1	
	Conocimiento y cumplimiento de los deberes en el tratamiento de datos personales.		
	Conocimiento de las sanciones y medidas de apremio contempladas en la LPDPPSOES.		
	Proceso general de atención de derechos ARCO.		
Físicas	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	B2.1.1	
	Los expedientes deben de estar en archiveros con llave.	B2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	B2.1.3	
Tecnológicas	Para ingresar al sistema se requiere proporcionar usuario y contraseña.	B3.1.1	
	El equipo de cómputo se encuentra protegido con acceso restringido a la red de Gobierno por antivirus y firewall.	B3.1.2	
	El Sistema Integral de Información Financiera tiene medidas de seguridad que limitan el acceso a las bases de datos.	B3.1.3	

1. Análisis de Riegos:

Medidas de seguridad actuales	ID	Riesgo / Amenaza	Factor de riesgo	Clasificación de riesgo	Control del factor	Valoración de riesgo	
						Impacto / probabilidad de que ocurra	Valor
B1.1.1	B1.2.1						
B2.1.1	B2.2.1						
B2.1.2	B2.2.2						
B2.1.3	B2.2.3						
B3.1.1	B3.2.1						
B3.1.2	B3.2.2						
B3.1.3	B3.2.3						

3. Análisis de Brecha:

Medidas de seguridad actuales	Riesgo	ID	Identificación de la brecha
B1.1.1	B1.2.1	B1.3.1	
B2.1.1	B2.2.1	B2.3.1	
B2.1.2	B2.2.2	B2.3.2	
B2.1.3	B2.2.3	B2.3.3	
B3.1.1	B3.2.1	B3.3.1	
B3.1.2	B3.2.2	B3.3.2	
B3.1.3	B3.2.3	B3.3.3	

4.- Plan de Trabajo:

Brecha que se atiende	Planificación				
	ID	Actividad	Responsable	Fecha tentativa	Evidencia / Entregable
B1.3.1	B1.4.1				
B2.3.1	B2.4.1				
B2.3.2	B2.4.2				
B2.3.3	B2.4.3				
B3.3.1	B3.4.1				
B3.3.2	B3.4.2				
B3.3.3	B3.4.3				

XII. Mecanismos de Monitoreo.

En términos de lo dispuesto por la LPDPPSOES, para la protección de datos personales, la CCS deberá establecer el monitoreo y revisión de manera periódica de las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que puedan estar sujetos los datos personales a su resguardo.

Para ello y con base en el plan de trabajo planteado por cada dirección, se estará solicitando a cada Dirección envíe a la Unidad de Transparencia copia de la evidencia que sustente las actividades realizadas; posteriormente, en la actualización anual que corresponda, se estará trabajando con las titulares de cada dirección, respecto a la efectividad de las medidas de seguridad implementadas, con la finalidad de evitar alteración, perdida o acceso no autorizado a los datos personales objeto de tratamiento.

XIII. Programa General de Capacitación.

La Unidad de Transparencia solicitará a la Secretaría de Transparencia y Rendición de Cuentas la capacitación del personal de la CCS que tenga entre sus actividades el tratamiento y resguardo de los datos personales.

XIV. Actualizaciones

De conformidad con lo establecido en el Artículo 47 de la LPDPPSOES, este documento de seguridad será actualizado cuando ocurra alguno de los siguientes eventos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que 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 una vulneración a la seguridad;
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

Estas modificaciones se realizarán y efectuarán, previa solicitud a la Unidad de Transparencia por parte de las unidades administrativas responsables de la protección de los datos personales.

Así mismo, como medida de actualización general, se establece que cuando se lleve a cabo la creación de un nuevo Aviso de Privacidad o Bases de Datos, el titular de la Dirección deberá dar aviso a la Unidad de Transparencia de la creación del nuevo aviso o base de datos, con el objeto de integrarlos al inventario de datos personales.

Aprobación

El presente documento fue aprobado por unanimidad de los integrantes del Comité de Transparencia de la Coordinación de Comunicación Social del Estado de Sinaloa en la Sesión Extraordinaria efectuada el día 17 de agosto de 2020.