



**COMISIÓN ESTATAL DE  
MEJORA REGULATORIA Y  
GESTIÓN EMPRESARIAL**



**SINALOA  
SECRETARÍA  
DE ECONOMÍA**



# **DOCUMENTO DE SEGURIDAD**

EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES EN  
POSESIÓN DE LA COMISIÓN ESTATAL DE MEJORA REGULATORIA Y  
GESTIÓN EMPRESARIAL

## Contenido

I.	Introducción.	4
II.	Marco Normativo.	6
	Objeto	7
A.	Responsable del Tratamiento de los Datos Personales y Fundamento para ello.	7
B.	Datos Sometidos a Tratamiento.	7
C.	Derechos de los Titulares de los Datos Personales.	8
D.	Área responsable de la implementación y observancia de esta política.	9
E.	Autorización – Consentimiento.	9
F.	Seguridad de los Datos Personales.	11
G.	Tratamiento de Datos Personales.	11
VI.	Inventarios de Datos Personales y de los Sistemas de Tratamiento	13
	Dirección de Gestión Empresarial	13
	Dirección de Reforma Regulatoria	18
	Coordinación Administrativa	20
	Unidad de Análisis Jurídico.	24
	Unidad de Transparencia	28
V.	Análisis de Riesgos.	35
VI.	Análisis de Brecha.	37
VII.	Plan de Trabajo.	37
VIII.	Metodología para la redacción y vinculación de la información.	38
	Dirección de Gestión Empresarial	38
	1. Medidas de Seguridad actuales:	38
	2. Análisis de Riesgos:	40
	3. Análisis de Brecha:	40
	4.- Plan de Trabajo:	40
	Dirección de Reforma Regulatoria	41
	1. Medidas de Seguridad actuales:	41

2. Análisis de Riegos: .....	42
3. Análisis de Brecha: .....	43
4.- Plan de Trabajo:.....	43
<b>Coordinación Administrativa.....</b>	<b>44</b>
1. Medidas de Seguridad actuales: .....	44
2. Análisis de Riegos: .....	45
3. Análisis de Brecha: .....	46
4.- Plan de Trabajo:.....	46
<b>Unidad de Análisis Jurídico .....</b>	<b>47</b>
1. Medidas de Seguridad actuales:.....	47
3. Análisis de Brecha: .....	49
4.- Plan de Trabajo:.....	49
<b>Unidad de Transparencia.....</b>	<b>50</b>
1. Medidas de Seguridad actuales: .....	50
2. Análisis de Riegos: .....	51
3. Análisis de Brecha: .....	52
<b>IX. Mecanismos de Monitoreo.....</b>	<b>54</b>
<b>X. Actualizaciones.....</b>	<b>54</b>
<b>Aprobación .....</b>	<b>55</b>

## 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 Comisión Estatal de Mejora Regulatoria y Gestión Empresarial (CEMERGE) 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 CEMERGE 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 coordinó la elaboración de 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 (LGPDPESO).
- Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa (LTAIPES).
- Ley Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sinaloa (LPDPPSOES).
- 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 LPDPPSOES, el presente documento es aplicable para todas las áreas de la CEMERGE, 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 Comisión Estatal de Mejora Regulatoria y Gestión Empresarial.**

La CEMERGE, 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 Comisión, 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 CEMERGE 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) Realización de trámites ante instancias municipales, estatales y/o federales y su seguimiento relacionadas con la apertura de empresas, regularización, trámites en problemas y canalización a programas de apoyos.
- b) Dichos datos también son utilizados para evaluar el servicio brindado a través de llamadas de calidad.
- c) Realizar solicitudes de servicios profesionales, requisiciones de materiales, efectuar pagos de facturas, así como celebrar contratos (no aplica para todos los proveedores).
- d) Realizar las consultas públicas de los Programas de Mejora Regulatoria (PMR), así como de la herramienta Análisis de Impacto Regulatorio (AIR) en el portal <http://urge.gob.mx>
- e) Interponer su Protesta Ciudadana en el portal <http://urge.gob.mx>

- f) Dar atención a su solicitud de ejercicio de derechos ARCO que se presente ante CEMERGE como responsable del tratamiento de los datos personales, así como con fines estadísticos.
- g) Recepción de solicitudes de acceso a la información
- h) Envío de información para promover servicios de la dependencia.

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

- 1) Nombre completo.
- 2) CURP
- 3) Razón Social
- 4) Sexo
- 5) Domicilio Fiscal de la empresa
- 6) Monto a invertir
- 7) Cantidad de empleos a generar
- 8) Número telefónico particular
- 9) Correo electrónico
- 10) Lugar y fecha de nacimiento
- 11) Estado Civil
- 12) Registro Federal de Contribuyentes
- 13) Edad.
- 14) Nivel de escolaridad.
- 15) Institución bancaria, número de cuenta y clave interbancaria.

### **C. Derechos de los Titulares de los Datos Personales.**

Para el ejercicio de cualquiera de los derechos Acceso, Rectificación, Cancelación y Oposición (ARCO) se deberá presentar la solicitud respectiva en la Comisión Estatal de Mejora Regulatoria y Gestión Empresarial, con domicilio en Blvd. Miguel

Tamayo Espinoza de los Monteros, Sección II Unidad de Servicios Estatales, Colonia Desarrollo Urbano Tres Ríos, Culiacán, Sinaloa, C.P. 80025.

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 2974; o bien ponerse en contacto con nuestro Responsable de la Unidad de Transparencia, que 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.

Los datos de contacto del Responsable de la Unidad de Transparencia son los siguientes: domicilio en Blvd. Miguel Tamayo Espinoza de los Monteros, Sección II Unidad de Servicios Estatales, Colonia Desarrollo Urbano Tres Ríos, Culiacán, Sinaloa, C.P. 80025. Teléfono (667)758-70-00 Extensión 2974.

#### **D. Área responsable de la implementación y observancia de esta política.**

La Unidad de Transparencia de CEMERGE 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 a 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 CEMERGE, 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 adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. La obligación y responsabilidad de la CEMERGE, se limita a disponer de los medios adecuados para este fin.

La CEMERGE, no garantiza la seguridad total de su información ni se responsabiliza por cualquier consecuencia derivada de 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 CEMERGE.

#### **G. Tratamiento de Datos Personales.**

La CEMERGE 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 CEMERGE.

#### **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 a continuación

- A. Dirección de Gestión Empresarial
- B. Dirección de Reforma Regulatoria.
- C. Coordinación Administrativa.
- D. Unidad de Análisis Jurídico.
- E. Unidad de Transparencia.

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 Gestión Empresarial**

**1.- Fundamento Legal.** - Capítulo Quinto, Artículo 33 del Reglamento Interior de la Comisión Estatal de Gestión Empresarial y Reforma Regulatoria.

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



### INVENTARIO DE DATOS PERSONALES GENERALES DIRECCION DE GESTIÓN EMPRESARIAL

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
<b>Datos de identificación y contacto</b>			
Nombre	X	X	
Alias			X
Seudónimo			X
Sexo	X	X	
Estado Civil	X	X	
Registro Federal de Contribuyentes (RFC)	X	X	
Registro Federal del Instituto Nacional (INE)			X
Clave Única de Registro de Población (CURP)	X	X	
Lugar de Nacimiento	X		X
Fecha de Nacimiento	X		X
Nacionalidad			X
Domicilio	X	X	
Teléfono particular	X		X
Teléfono celular personal	X	X	
Correo electrónico personal	X	X	
Firma autógrafa	X	X	
Firma electrónica			
Edad			
Fotografía			
Referencias personales			
Escolaridad	X		X
Numero de seguridad social o análogo			X
<b>Datos sobre características físicas</b>			
Color de piel			X
Color de cabello			X
Señas particulares			X
Estatura			X
Peso			X
Cicatrices			X
Tipo de sangre			X

Datos biomédicos			
Datos Personales Recabados	Existente	Necesario	No necesario
Imagen de iris			X
Huella dactilar			X
Palma de la mano			X
ADN (Código genético)			
Datos laborales			
Puesto o cargo que desempeña			X
Domicilio del trabajo	X	X	
Correo electrónico institucional	X	X	
Teléfono institucional	X	X	
Referencia laborales			X
Información generada durante los procedimientos de reclutamiento, selección y contratación			X
Experiencia/Capacitación laboral			X
Datos académicos			
Trayectoria educativa			X
Títulos			X
Cedula profesional			X
Certificados			X
Reconocimientos			X
Datos migratorios			
Entrada al país			X
Salida de país			X
Tiempo de permanencia en el país			X
Calidad migratoria			X
Derechos de residencia			X
Aseguramiento			X
Repatriación			X
Datos patrimoniales y/o financieros			
Bienes muebles			X
Bienes inmuebles			X
Información fiscal			X
Historial crediticio/Buró de crédito			X
Ingresos			X
Egresos			X
Cuentas bancarias			X
Números de tarjetas de crédito			X
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			X

Seguros			X
Afores			X
<b>Datos sobre pasatiempos, entretenimientos y diversión</b>			
Datos Personales Recabados	Existente	Necesario	No necesario
Pasatiempos			X
Aficiones			X
Deportes de practica			X
Juegos de su interés			X
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			X
Otros datos personales (mencionar)			
Razón social	X	X	
Monto de inversión	X	X	
Cantidad de empleos a generar (permanentes y eventuales)	X	X	

Área: DIRECCIÓN DE GESTIÓN EMPRESARIAL

**INVENTARIO DE DATOS PERSONALES SENSIBLES**  
DIRECCION DE GESTIÓN EMPRESARIAL

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
<b>Datos de identificación y contacto</b>			
Posturas religiosas/ideológicas/morales/filosóficas			X
Pertenencia a un partido/Posturas políticas			X
Pertenencia a un sindicato			X
<b>Datos de Salud</b>			
Estado de salud físico presente, pasado o futuro			X
Estado de salud mental presente, pasado o futuro			X
Información genética			X
<b>Datos sobre vida sexual</b>			
Preferencias sexuales			X
Prácticas o hábitos sexuales			X
<b>Datos de origen étnicos o racial</b>			
Pertenencia a un pueblo, etnia o región			X
<b>Datos Familiares</b>			
Relaciones afectivas, familiares y conyugales			X
<b>Otros datos personales (mencionar)</b>			

Area: DIRECCIÓN DE GESTIÓN EMPRESARIAL

**3.- Forma de obtención de los datos personales.** - se obtienen mediante un formulario físico y electrónico.

**4.- Servidor Público Administrador de la Dirección:**

Cargo: Directora de Gestión Empresarial

Teléfono y Extensión: 667 758-7000 Ext 2692

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Reglamento Interior de la CEGERR, y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, Coordinar la Red de Unidades Rápida de Gestión Empresarial en el Estado, para brindar una atención especializada, integral y de calidad a los particulares, a través de los instrumentos de gestión y asesoría de trámites vigentes, así como de los programas federales, estatales y municipales de apoyo a las empresas.

**5.- Tipo de Soporte.** - El soporte de los Datos Personales se encuentra el Físico y electrónico

**6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales.** - La Dirección de Gestión Empresarial se encuentra en Blvd. Miguel Tamayo Espinoza de los Monteros, Unidad de Servicios Estatales, Desarrollo Urbano Tres Ríos, Culiacán, Sinaloa, los Archivos físicos y electrónicos se encuentran en una oficina con acceso restringido y están depositados en archiveros con llave, también se resguarda información de datos personales en bodega rentada por esta Comisión, así como en las oficinas de las Unidades Rápidas de Gestión Empresarial (URGE) instaladas en los 18 municipios.

**7.- Portabilidad de datos.** - La Dirección de Gestión Empresarial no cuenta con ningún formato estructurado para la portabilidad de datos.

**8.- Transferencia de datos.** - La Dirección de Gestión Empresarial transfiere los datos personales a la instancia correspondiente para la realización del trámite o servicio.

**9.- Encargado de datos.** - Dirección de Gestión Empresarial

## Dirección de Reforma Regulatoria

**1.- Fundamento Legal.** - Sección II, artículo 35 del Reglamento Interior de la Comisión Estatal de Gestión Empresarial y Reforma Regulatoria.

**2.- Datos Personales que se encuentran en la Dirección:** Esta dirección cuenta con un aviso de privacidad que corresponde a la Consulta Pública de los Programas de Mejora Regulatoria, así como la herramienta Análisis de Impacto Regulatorio (AIR) en el portal <http://urges.gob.mx>.



### INVENTARIO DE DATOS PERSONALES GENERALES DIRECCIÓN DE MEJORA REGULATORIA

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

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



**INVENTARIO DE DATOS PERSONALES SENSIBLES  
DIRECCIÓN DE MEJORA REGULATORIA**

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

Datos personales recabados	Existente	Necesario	No necesario
<b>Datos de identificación y contacto</b>			
Posturas religiosas/ ideológicas/morales/filosóficas			X
Pertenencia a un partido/Posturas políticas			X
Pertenencia a un sindicato			X
<b>Datos de Salud</b>			
Estado de salud físico presente, pasado o futuro			X
Estado de salud mental presente, pasado o futuro			X
Información genética			X
<b>Datos sobre vida sexual</b>			
Preferencias sexuales			X
Prácticas o hábitos sexuales			X
<b>Datos de origen étnicos o racial</b>			
Pertenencia a un pueblo, etnia o región			X
<b>Datos Familiares</b>			
Relaciones afectivas, familiares y conyugales			
<b>Otros datos personales (mencionar)</b>			
			X

Área: Dirección de Mejora Regulatoria

**3.- Forma de obtención de los datos personales.** - se obtienen mediante portal institucional.

**4.- Servidor Público Administrador de la Dirección:**

Cargo: Directora de Reforma Regulatoria

Teléfono y Extensión: 667 758-70-00 Ext 2693

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Reglamento Interior de la CEGERR, y realizar aquellas que le encomienden sus superiores jerárquicos.

- I. Obligaciones: Entre otras Coordinar el Programa de Reforma Regulatoria a corto, mediano y largo plazo;

- II. Coordinar la elaboración de un programa de Reforma Regulatoria en las Dependencias, Estatales, así como en el ámbito municipal;
- III. Crear programas innovadores de simplificaciones de trámites y servicios;
- IV. Integrar y actualizar el Registro Sinaloense de Trámites y Servicios;
- V. Implementar y coordinar el Registro de Personas Acreditadas;
- VI. Brindar asesoría técnica y capacitación en materia de Reforma Regulatoria a las dependencias Estatales y Municipales;
- VII. Revisar, dictaminar y capacitar sobre la elaboración de la Manifestación de Impacto Regulatorio a las dependencias estatales, así como cualquier nueva regulación que emitan las mismas;

Cumplir cabalmente con el Código de Ética y Código de Conducta de la Comisión;

**5.- Tipo de Soporte.** - El soporte de los Datos Personales se encuentran en físico.

**6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales.** - La Dirección de Reforma Regulatoria se encuentra en Blvd. Miguel Tamayo Espinoza de los Monteros, Unidad de Servicios Estatales, Desarrollo Urbano Tres Ríos, Culiacán, Sinaloa. Los Archivos físicos se encuentran en una oficina con acceso restringido y están depositados en archiveros con llave.

**7.- Portabilidad de datos.** - La Dirección de Reforma Regulatoria no cuenta con ningún formato estructurado para la portabilidad de datos.

**8.- Transferencia de datos.** - La Dirección de Reforma Regulatoria no transfiere los datos personales.

**9.- Encargado de datos.** - La Dirección de Reforma Regulatoria.

## **Coordinación Administrativa**

**1.- Fundamento Legal.** - Capítulo VI, 1.1.2. del Manual de Organización de la Comisión Estatal de Gestión Empresarial y Reforma Regulatoria.

**2.-Datos Personales que se encuentran en la Coordinación:** Esta dirección cuenta con un aviso de privacidad donde se recaban datos personales con la finalidad de realizar solicitudes de servicios profesionales, requisiciones de

materiales, efectuar pagos de facturas, así como celebrar contratos (no aplica para todos los proveedores).



**INVENTARIO DE DATOS PERSONALES GENERALES  
COORDINACIÓN ADMINISTRATIVA**

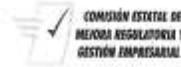
Marque con una **X** los datos personales que existen y son necesarios o que existen más no son necesarios en los procesos o trámites llevados a cabo en su Unidad Administrativa.

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

Tipo de sangre			X
<b>Datos biomédicos</b>			
<b>Datos Personales Recabados</b>	<b>Existente</b>	<b>Necesario</b>	<b>No necesario</b>
Imagen de iris			X
Huella dactilar			X
Palma de la mano			X
ADN (Código genético)			X
<b>Datos laborales</b>			
Puesto o cargo que desempeña	X	X	
Domicilio del trabajo	X	X	
Correo electrónico institucional	X	X	
Teléfono institucional	X	X	
Referencia laborales			X
Información generada durante los procedimientos de reclutamiento; selección y contratación			X
Experiencia/Capacitación laboral	X	X	
<b>Datos académicos</b>			
Trayectoria educativa	X	X	
Títulos	X	X	
Cedula profesional	X		X
Certificados	X		X
Reconocimientos	X		X
<b>Datos migratorios</b>			
Entrada al país			X
Salida de país			X
Tiempo de permanencia en el país			X
Calidad migratoria			X
Derechos de residencia			X
Aseguramiento			X
Repatriación			X
<b>Datos patrimoniales y/o financieros</b>			
Bienes muebles			X
Bienes inmuebles			X
Información fiscal			X
Historial crediticio/Buró de crédito			X
Ingresos			X
Egresos			X
Cuentas bancarias	X	X	
Números de tarjetas de crédito			X
Información adicional de tarjeta (fechas)			X

2

de vencimiento, códigos de seguridad, datos de banda magnética, pin)			X
Seguros			X
Afores			X
<b>Datos sobre pasatiempos, entretenimientos y diversión</b>			
<b>Datos Personales Recabados</b>	<b>Existente</b>	<b>Necesario</b>	<b>No necesario</b>
Pasatiempos			X
Aficiones			X
Deportes de practica			X
Juegos de su interés			X
<b>Datos legales</b>			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)	X	X	
<b>Otros datos personales (mencionar)</b>			



**INVENTARIO DE DATOS PERSONALES SENSIBLES  
COORDINACIÓN ADMINISTRATIVA**

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
<b>Datos de identificación y contacto</b>			
Posturas religiosas/ideológicas/morales/filosóficas			X
Pertenencia a un partido/Posturas políticas			X
Pertenencia a un sindicato			X
<b>Datos de Salud</b>			
Estado de salud físico presente, pasado o futuro	X	X	
Estado de salud mental presente, pasado o futuro			X
Información genética			X
<b>Datos sobre vida sexual</b>			
Preferencias sexuales			X
Prácticas o hábitos sexuales			X
<b>Datos de origen étnicos o racial</b>			
Pertenencia a un pueblo, etnia o región			X
<b>Datos Familiares</b>			
Relaciones afectivas, familiares y conyugales			X
<b>Otros datos personales (mencionar)</b>			

**3.- Forma de obtención de los datos personales.** - se obtienen mediante un formulario físico y electrónico.

**4.- Servidor Público Administrador de la Coordinación:**

Cargo: Coordinadora Administrativa

Teléfono y Extensión: 667 758-70-00 Ext. 2690

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Manual de Organización de la CEGERR, y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, realizar solicitudes de servicios profesionales, requisiciones de materiales, efectuar pagos de facturas, así como celebrar contratos (no aplica para todos los proveedores).

**5.- Tipo de Soporte.** - El soporte de los Datos Personales se encuentran en físico.

**6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales.** - La Coordinación Administrativa se encuentra en Blvd. Miguel Tamayo Espinoza de los Monteros, Unidad de Servicios Estatales, Desarrollo Urbano Tres Ríos, Culiacán, Sinaloa. Los Archivos físicos se

encuentran en una oficina con acceso restringido y están depositados en archiveros con llave.

**.7.- Portabilidad de datos.** - La Coordinación Administrativa no cuenta con ningún formato estructurado para la portabilidad de datos.

**8.- Transferencia de datos.** - La Coordinación Administrativa no transfiere los datos personales.

**9.- Encargado de datos.** - La Coordinación Administrativa.

### **Unidad de Análisis Jurídico.**

**1.- Fundamento Legal.** – Capítulo VI, 1.1.4 del Manual de Organización de la Comisión Estatal de Gestión Empresarial y Reforma Regulatoria.

#### **2.-Datos Personales que se encuentran en la Unidad:**

En esta unidad se manejan dos avisos de privacidad donde se recaban datos personales, el primero es para interponer la Protesta Ciudadana y el segundo para la Queja por Obstrucción Empresarial.



**INVENTARIO DE DATOS PERSONALES GENERALES  
UNIDAD DE ANÁLISIS JURÍDICO**

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
<b>Datos de identificación y contacto</b>			
Nombre	x	X	
Alias			X
Seudónimo			X
Sexo			X
Estado Civil			X
Registro Federal de Contribuyentes (RFC)			X
Registro Federal del instituto Nacional (INE)			x
Clave Unica de Registro de Población (CURP)			X
Lugar de Nacimiento			X
Fecha de Nacimiento		X	
Nacionalidad			X
Domicilio			X
Teléfono particular	x	X	
Teléfono celular personal			
Correo electrónico personal	x	X	
Firma autógrafa			X
Firma electrónica			X
Edad		X	
Fotografía			X
Referencias personales			X
Escolaridad			X
Número de seguridad social o análogo			X
<b>Datos sobre características físicas</b>			
Color de piel			X
Color de cabello			X
Señas particulares			X
Estatura			X
Peso			X
Cicatrices			X
Tipo de sangre			X

Datos biomédicos			
Datos Personales Recabados	Existente	Necesario	No necesario
Imagen de iris		X	
Huella dactilar			X
Palma de la mano			X
ADN (Código genético)			X
Datos laborales			
Puesto o cargo que desempeña			X
Domicilio del trabajo		X	
Correo electrónico institucional			X
Teléfono institucional		X	
Referencia laborales			X
Información generada durante los procedimientos de reclutamiento; selección y contratación			X
Experiencia/Capacitación laboral			X
Datos académicos			
Trayectoria educativa			X
Títulos			X
Cedula profesional			X
Certificados			X
Reconocimientos			X
Datos migratorios			
Entrada al país			X
Salida de país			X
Tiempo de permanencia en el país			X
Calidad migratoria			X
Derechos de residencia			X
Aseguramiento			X
Repatriación			X
Datos patrimoniales y/o financieros			
Bienes muebles			X
Bienes inmuebles			X
Información fiscal			X
Historial crediticio/Buro de crédito			X
Ingresos			X
Egresos			X
Cuentas bancarias			X
Números de tarjetas de crédito			X
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			X

3

Seguros			X
Mores			X
<b>Datos sobre pasatiempos, entretenimientos y diversión</b>			
Datos Personales Recabados	Existente	Necesario	No necesario
Pasatiempos			X
Aliciones			X
Deportes de practica			X
Juegos de su interés			X
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			X
Otros datos personales (mencionar)			
Narración de hechos (protesta ciudadana)			



**INVENTARIO DE DATOS PERSONALES SENSIBLES  
UNIDAD DE ANÁLISIS JURÍDICO**

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
<b>Datos de identificación y contacto</b>			
Posturas religiosas/ideológicas/morales/filosóficas			X
Pertenencia a un partido político			X
Pertenencia a un sindicato			X
<b>Datos de Salud</b>			
Estado de salud físico presente, pasado o futuro			X
Estado de salud mental presente, pasado o futuro			X
Información genética			X
<b>Datos sobre vida sexual</b>			
Preferencias sexuales			X
Prácticas o hábitos sexuales			X
<b>Datos de origen étnico o racial</b>			
Pertenencia a un pueblo, etnia o región			X
<b>Datos Familiares</b>			
Relaciones afectivas, familiares y conyugales			X
<b>Otros datos personales (mencionar)</b>			
Nombre			

**3.- Forma de obtención de los datos personales.** - se obtienen mediante un formulario físico y formulario electrónico.

**4.- Servidor Público Administrador de la Unidad:**

Cargo: Titular de Unidad de Análisis Jurídico

Teléfono y Extensión: 667 758-7000 Ext. 2971

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Manual de Organización de la CEGERR, y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Entre otras, Otorgar apoyo al personal de la Comisión en el cumplimiento de sus obligaciones, así como, dar asesoría jurídica a los empresarios.

## Unidad de Transparencia

**1.- Fundamento Legal.** - Capítulo Cuarto, fracción V del Acuerdo que reforma y adiciona el Reglamento Interior de la Comisión Estatal de Gestión Empresarial y Reforma Regulatoria.

**2.- Datos Personales que se encuentran en la Unidad:** Esta unidad cuenta con un aviso de privacidad para la recepción de solicitudes de información y ejercicio de los derechos ARCO.



### INVENTARIO DE DATOS PERSONALES GENERALES UNIDAD DE TRANSPARENCIA

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
<b>Datos de identificación y contacto</b>			
Nombre	X		X
Alias	X		X
Seudónimo	X		X
Sexo			
Estado Civil			X
Registro Federal de Contribuyentes (RFC)			x
Registro Federal del instituto Nacional (INE)	x	x	
Clave Única de Registro de Población (CURP)			x
Lugar de Nacimiento			x
Fecha de Nacimiento			x
Nacionalidad			x
Domicilio			x
Teléfono particular	x	x	
Teléfono celular personal	X	x	
Correo electrónico personal	X	x	
Firma autógrafa	x	x	
Firma electrónica			x
Edad			x
Fotografía			x
Referencias personales			x
Escolaridad			x
Número de seguridad social o análogo			x
<b>Datos sobre características físicas</b>			
Color de piel			X
Color de cabello			X
Señas particulares			X
Estatura			X
Peso			X
Cicatrices			X
Tipo de sangre			X

<b>Datos biomédicos</b>			
<b>Datos Personales Recabados</b>	<b>Existente</b>	<b>Necesario</b>	<b>No necesario</b>
Imagen de iris			X
Huella dactilar			X
Palma de la mano			X
ADN (Código genético)			X
<b>Datos laborales</b>			
Puesto o cargo que desempeña			X
Domicilio del trabajo			X
Correo electrónico institucional			X
Teléfono institucional			X
Referencia laborales			X
Información generada durante los procedimientos de reclutamiento, selección y contratación			X
Experiencia/Capacitación laboral			X
<b>Datos académicos</b>			
Trayectoria educativa			X
Titulos			X
Cedula profesional			X
Certificados			X
Reconocimientos			X
<b>Datos migratorios</b>			
Entrada al país			X
Salida de país			X
Tiempo de permanencia en el país			X
Calidad migratoria			X
Derechos de residencia			X
Aseguramiento			X
Repatriación			X
<b>Datos patrimoniales y/o financieros</b>			
Bienes muebles			X
Bienes inmuebles			X
Información fiscal			X
Historial crediticio/Buró de crédito			X
Ingresos			X
Egresos			X
Cuentas bancarias			X
Números de tarjetas de crédito			X
Información adicional de tarjeta (fechas de vencimiento, códigos de seguridad, datos de banda magnética, pin)			X

Seguros			X
Afores			X
<b>Datos sobre pasatiempos, entretenimientos y diversión</b>			
<b>Datos Personales Recabados</b>	<b>Existente</b>	<b>Necesario</b>	<b>No necesario</b>
Pasatiempos			X
Aficiones			X
Deportes de practica			X
Juegos de su interés			X
<b>Datos legales</b>			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			X
<b>Otros datos personales (mencionar)</b>			



**INVENTARIO DE DATOS PERSONALES SENSIBLES  
UNIDAD DE TRANSPARENCIA**

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
<b>Datos de identificación y contacto</b>			
Posturas religiosas/ideológicas/morales/filosóficas			X
Pertenencia a un partido/Posturas políticas			X
Pertenencia a un sindicato			X
<b>Datos de Salud</b>			
Estado de salud físico presente, pasado o futuro			X
Estado de salud mental presente, pasado o futuro			X
Información genética			X
<b>Datos sobre vida sexual</b>			
Preferencias sexuales			X
Prácticas o hábitos sexuales			X
<b>Datos de origen étnicos o racial</b>			
Pertenencia a un pueblo, etnia o región			X
<b>Datos Familiares</b>			
Relaciones afectivas, familiares y conyugales			X
<b>Otros datos personales (mencionar)</b>			

**4.- Servidor Público Administrador de la Unidad:**

Cargo: Responsable de Unidad de Transparencia.

Teléfono y Extensión: 667 758-7000 Ext. 2974

Funciones/Perfil: Cumplir con las funciones que correspondan al puesto de conformidad con el Manual de Organización de CEMERGE, y realizar aquellas que le encomienden sus superiores jerárquicos.

Obligaciones: Recabar y difundir la información a que se refieren las obligaciones de transparencia que le competan de conformidad con la Ley General de Transparencia y Acceso a la Información Pública y la Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa, así como propiciar que las áreas las actualicen periódicamente, conforme la normatividad aplicable.

**5.- Tipo de Soporte.** - El soporte de los Datos Personales se encuentra en físico y electrónico.

**6.- Características del lugar donde se resguardan los sistemas de tratamiento de datos personales.** - La Unidad de Transparencia se encuentra en Blvd. Miguel Tamayo Espinoza de los Monteros, Unidad de Servicios Estatales,

Desarrollo Urbano Tres Ríos, Culiacán, Sinaloa. Los Archivos físicos se encuentran en una oficina con acceso restringido y están depositados en archiveros con llave.

**7.- Portabilidad de datos.** – La Unidad de Transparencia no cuenta con ningún formato estructurado para la portabilidad de datos.

**8.- Transferencia de datos.** – La Unidad de Transparencia no transfiere los datos personales.

**9.- Encargado de datos.** - La Unidad de Transparencia.

## **X.- 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, en 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 abordarán 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 CEMERGE, cuenta con las siguientes:

**De Tipo Físico:**

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

Para lo anterior, la CEMERGE se encuentra dentro de las instalaciones de la Unidad de Servicios Estatales (USE), 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 CEMERGE.

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 CEMERGE, 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 socio-organizativos (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 CEMERGE se cuenta con acciones y mecanismos que permiten proteger e identificar los equipos móviles y portátiles; mobiliario, documentos y materiales.

- 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 CEMERGE 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 respectivo.

- 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 con son Fireworks, 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.

## **V. Análisis de Riesgos.**

En el establecimiento de las medidas de seguridad, se debe 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 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 a cabo 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 pueden ser:	
TIC	Tecnologías de la información y comunicación. (Software y Hardware)
Capacitación	Desconocimiento de los Procesos.
Control	Falta de control.
Recursos	Humanos, financieros, materiales.

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

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. Medio=2	8	Rojo	
	P. de O. Bajo=1	7	Rojo	
Impacto Medio =2	P. de O. Alto=3	6	Naranja	
	P. de O. Medio=2	5	Naranja	
	P. de O. Bajo=1	4	Naranja	
Impacto Bajo =1	P. de O. Alto=3	3	Amarillo	
	P. de O. Medio=2	2	Amarillo	
	P. de O. Bajo=1	1	Amarillo	

## VI. 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.

## VII. Plan de Trabajo.

Una vez realizado en análisis de riesgo y el análisis de brecha, cada dirección elaboro 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.

## VIII. 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 dígito:** Empieza con una letra Mayúscula que corresponde a una Dirección de la CEMERGE.

**Segundo dígito:** Continúa con un número consecutivo del sistema de tratamiento de datos personales.

**Tercer dígito:** 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 en número 1, para los riesgos o amenazas, se utiliza en número 2, al describir las brechas se utiliza en número 3 y la referencia del plan de trabajo, se hace con el número 4.

**Cuarto dígito:** 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.

### Dirección de Gestión Empresarial

#### 1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
ADMINISTRATIVAS	Políticas interna de protección de datos personales.	A1.1.1	
	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.		

<b>FISICAS</b>	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	A2.1.1	
	Los expedientes deben de estar en archiveros con llave.	A2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	A2.1.3	

<b>TECNOLÓGICAS</b>	Para ingresar al equipo de cómputo se necesita proporcionar usuario y contraseña.	A3.1.1	
---------------------	---	--------	--

## 2. Análisis de Riesgos:

Medida de seguridad actuales	ID	Riesgo/amenaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidad de que ocurra	valor
A1.1.1	A1.2.1						
A2.1.1	A2.2.1						
A2.1.2	A2.2.2						
A2.1.3	A2.2.3						

## 3. Análisis de Brecha:

Medida de seguridad actuales	Riesgos	ID	Identificación de la Brecha
A1.1.1	A1.2.1	A1.3.1	
A2.1.1	A2.2.1	A2.3.1	
A2.1.2	A2.2.2	A2.3.2	
A2.1.3	A2.2.3	A2.3.3	

## 4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	

A1.3.1	A1.4. 1				
A2.3.1	A2.4. 1				
A2.3.2	A2.4. 2				
A2.3.3	A2.4. 3				

## Dirección de Reforma Regulatoria

### 1. Medidas de Seguridad actuales:

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.		
FISICAS	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

## 2. Análisis de Riesgos:

Medida de seguridad actuales	ID	Riesgo/amenaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidades 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:

Medida de seguridad actuales	Riesgos	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	

### 4.- Plan de Trabajo:

Brecha que se Atiende	Planificación			Evidencia/Entregable
	ID	Actividad	Responsable	
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				

## Coordinación Administrativa

### 1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
<b>ADMINISTRATIVAS</b>	Políticas interna de protección de datos personales.	C1.1.1	
	Conocimiento y cumplimiento de los deberes en el tratamiento de datos personales.		
	Conocimiento de las sanciones y medidas de apremio contempladas en la LPDPPSOES.		
<b>FISICAS</b>	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	C2.1.1	

	Los expedientes deben de estar en archiveros con llave.	C2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	C2.1.3	

<b>TECNOLÓGICAS</b>			
	Para ingresar al equipo de cómputo se necesita proporcionar usuario y contraseña.	C3.1.1	

## 2. Análisis de Riesgos:

Medida de seguridad actuales	ID	Riesgo/amenaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidad de que ocurra	valor
C1.1.1	C1.2.1						
C2.1.1	C2.2.1						

C2.1.2	C2.2.2						
C2.1.3	C2.2.3						

### 3. Análisis de Brecha:

Medida de seguridad actuales	Riesgos	ID	Identificación de la Brecha
C1.1.1	C1.2.1	C1.3.1	
C2.1.1	C2.2.1	C2.3.1	
C2.1.2	C2.2.2	C2.3.2	
C2.1.3	C2.2.3	C2.3.3	

### 4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
C1.3.1	C1.4.1				
C2.3.1	C2.4.1				

C2.3.2	C2.4.2				
C2.3.3	C2.4.3				

## Unidad de Análisis Jurídico

### 1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
<b>ADMINISTRATIVAS</b>	Políticas interna de protección de datos personales.	D1.1.1	
	Conocimiento y cumplimiento de los deberes en el tratamiento de datos personales.		
	Conocimiento de las sanciones y medidas de apremio contempladas en la LPDPPSOES.		
<b>FISICAS</b>	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	D2.1.1	
	Los expedientes deben de estar en archiveros con llave.	D2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	D2.1.3	
<b>TECNOLOGICAS</b>	Para ingresar al equipo de cómputo se necesita proporcionar usuario y contraseña.	D3.1.1	

	El equipo de cómputo se encuentra protegido con acceso restringido a la red de gobierno, por antivirus y Fireworks.	D3.1.2	
--	---	--------	--

## 2. Análisis de Riegos:

Medida de seguridad actuales	ID	Riesgo/amenaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidad de que ocurra	valor
D1.1.1	D1.2.1						
D2.1.1	D2.2.1						
D2.1.2	D2.2.2						
D2.1.3	D2.2.3						
D3.1.1	D3.2.1						
D3.1.2	D3.2.2						

### 3. Análisis de Brecha:

Medida de seguridad actuales	Riesgos	ID	Identificación de la Brecha
D1.1.1	D1.2.1	D1.3.1	
D2.1.1	D2.2.1	D2.3.1	
D2.1.2	D2.2.2	D2.3.2	
D2.1.3	D2.2.3	D2.3.3	
D3.1.1	D3.2.1	D3.3.1	
D3.1.2	D3.2.2	D3.3.2	

### 4.- Plan de Trabajo:

Brecha que se Atiende	Planificación				Evidencia/Entregable
	ID	Actividad	Responsable	Fecha Tentativa	
D1.3.1	D1.4.1				
D2.3.1	D2.4.1				
D2.3.2	D2.4.2				

D2.3.3	D2.4.3				
D3.3.1	D3.4.1				
D3.3.2	D3.4.2				

### Unidad de Transparencia.

#### 1. Medidas de Seguridad actuales:

TIPO	CONTROL/MECANISMO	ID	MEDIDAS ACTUALES
<b>ADMINISTRATIVAS</b>	Políticas interna de protección de datos personales.	E1.1.1	
	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.		
<b>FISICAS</b>	Prevenir el Acceso no autorizado a la oficina donde se tienen resguardados los datos personales.	E2.1.1	

	Los expedientes deben de estar en archiveros con llave.	E2.1.2	
	No dejar expedientes sobre el escritorio si no se están utilizando.	E2.1.3	
<b>TECNOLOGICAS</b>	Para ingresar al equipo de cómputo se necesita proporcionar usuario y contraseña.	E3.1.1	
	El equipo de cómputo se encuentra protegido con acceso restringido a la red de gobierno, por antivirus y Fireworks.	E3.1.2	

## 2. Análisis de Riegos:

Medida de seguridad actuales	ID	Riesgo/am enaza	Factor de Riesgo	Clasificación del Riesgo	Control del Factor	Valoración de Riesgo	
						Impacto/probabilidad de que ocurra	valor
E1.1.1	E1.2.1						
E2.1.1	E2.2.1						
E2.1.2	E2.2.2						

E2.1.3	E2.2.3						
E3.1.1	E3.2.1						
E3.1.2	E3.2.2						

### 3. Análisis de Brecha:

Medida de seguridad actuales	Riesgos	ID	Identificación de la Brecha
E1.1.1	E1.2.1	E1.3.1	
E2.1.1	E2.2.1	E2.3.1	
E2.1.2	E2.2.2	E2.3.2	
E2.1.3	E2.2.3	E2.3.3	
E3.1.1	E3.2.1	E3.3.1	
E3.1.2	E3.2.2	E3.3.2	

### 4.- Plan de Trabajo:

Brecha	Planificación	Evidencia/Entregabl
--------	---------------	---------------------

que se Atiende	ID	Actividad	Responsable	Fecha Tentativa	e
E1.3.1	E1.4. 1				
E2.3.1	E2.4. 1				
E2.3.2	E2.4. 2				
E2.3.3	E2.4. 3				
E3.3.1	E3.4. 1				
E3.3.2	E3.4. 2				

## **IX. Mecanismos de Monitoreo.**

En términos de lo dispuesto por la LPDPPSOES, para la protección de datos personales, la CEMERGE 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 envié 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, pérdida o acceso no autorizado a los datos personales objeto de tratamiento.

## **X. 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.

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 mayoría de votos de los integrantes del Comité de Transparencia de la Comisión Estatal de Mejora Regulatoria y Gestión Empresarial, en la II Sesión Ordinaria efectuada el día 14 de Agosto de 2020.

**ACTA DE SEGUNDA SESIÓN DEL COMITÉ DE TRANSPARENCIA DE LA COMISIÓN ESTATAL DE MEJORA REGULATORIA Y GESTIÓN EMPRESARIAL QUE APRUEBA EL CALENDARIO DE SESIONES Y EL DOCUMENTO DE SEGURIDAD EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES EN POSESIÓN DE LA COMISIÓN ESTATAL DE MEJORA REGULATORIA Y GESTIÓN EMPRESARIAL**

En la Ciudad de Culiacán Rosales, Sinaloa, siendo las 13:00 horas del día 14 de Agosto del año 2020 (dos mil veinte), a través de la plataforma virtual Zoom en esta Ciudad capital; reunidos para celebrar formalmente segunda Sesión del Comité de Transparencia de esta Comisión, con el fin de aprobar el calendario de sesiones y el Documento de Seguridad en Materia de Tratamiento de Datos Personales en Posesión de la CEMERGE; Con fundamento en lo dispuesto por el artículo 111 fracciones I y II, de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Sinaloa, se reúnen los integrantes del Comité de Transparencia, **Lic. Kaleoppy Ornelas Cárdenas**, Directora de Mejora Regulatoria y Presidenta del Comité de Transparencia, **Lic. Perla Vanessa Ortiz Navarrete**, Directora de Gestión Empresarial y miembro del Comité de Transparencia, así como **la Lic. Ruth Ayame Saito Murguía**, en calidad de miembros;

**CONSIDERANDO**

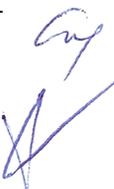
Que la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Sinaloa, establece que el Comité de Transparencia es aquella instancia a la que hace referencia el artículo 61 de la Ley de Transparencia y Acceso a la Información Pública y dicho artículo dice que es el órgano colegiado que se integrará en cada uno de los sujetos obligados que deberá de estar integrado por un número impar de servidores públicos y, en su caso, de personas designadas por su Titular.

Que el Comité de Transparencia en su calidad de órgano revisor, adoptará en forma colegiada sus resoluciones por unanimidad o mayoría de votos. En caso de empate el Presidente tendrá voto de calidad.

Que la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Sinaloa puntualiza que el Comité de Transparencia será la autoridad máxima en materia de protección de datos personales, en la organización del responsable

Que una de las facultades del Comité de Transparencia es la de aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la Ley de Protección de Datos Personales y demás disposiciones que resulten aplicables a la materia. Asimismo, es potestad del mismo Comité el coordinar, realizar y supervisar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable.

Que sobre las consideraciones anteriores y en observancia a lo que establecen las Leyes previamente mencionadas, el Responsable de la Unidad de Transparencia señala que la Unidad de Transparencia, se encuentra en constante actualización del "Documento de Seguridad en Materia de Tratamiento de Datos Personales en Posesión de Comisión Estatal de Mejora Regulatoria y Gestión Empresarial" y a petición expresa de las unidades administrativas responsables de la Protección de Datos Personales se incorporan nuevos elementos relativos a temas de responsabilidades administrativas y auditoría de esta Comisión, lo anterior de acuerdo a las fracciones 1 y 11 del artículo 111 de la Ley de Protección de Datos Personales debe de ser aprobado por el Comité de Transparencia.





Así pues, el documento a aprobar aduce que 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".

Sigue manifestando que a partir de la publicación de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Sinaloa y los Lineamientos de Protección de Datos Personales para Sujetos Obligados del Estado de Sinaloa, CEMERGE 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. -Que entre los "Deberes" previstos en la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Sinaloa, CEMERGE deberá de 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 coordinó la elaboración de dicho documento, para cumplir con los que se establece en los artículos 35 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 42 de la Ley de Protección de Datos Personales local.

Que, tras analizar las modificaciones del Documento de Seguridad en Materia de Tratamiento de Datos Personales en Posesión de la CEMERGE, es procedente aprobarlo en su totalidad.

Que este Comité de Transparencia como órgano colegiado, en uso de las funciones establecidas en el artículo 111, fracciones 1 y 11 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Sinaloa, por unanimidad resuelve emitir los siguientes:

#### **ACUERDOS**

**PRIMERO.** - Se aprueba el Documento de Seguridad en Materia de Tratamiento de Datos Personales en Posesión de la CEMERGE, aplicando las observaciones realizadas por los miembros del comité en primera sesión ordinaria.

**SEGUNDO.** - Se instruye al Titular de la Unidad de Transparencia de la CEMERGE dar a conocer a los servidores públicos adscritos a esta Comisión el documento aprobado y manifestarles la importancia de su observación y cumplimiento.

**TERCERO.** - Se aprueba el calendario de sesiones ordinarias propuesto, quedando de la siguiente manera:

**III Sesión Ordinaria** 15 de Octubre

**IV Sesión Ordinaria** 15 de Diciembre del año en curso.



**COMISIÓN ESTATAL DE  
MEJORA REGULATORIA Y  
GESTIÓN EMPRESARIAL**



**SINALOA  
SECRETARÍA  
DE ECONOMÍA**



Lo anterior se acordó por mayoría de votos del Comité de Transparencia de esta Comisión, en la ciudad de Culiacán de Rosales, Sinaloa a los 14 días del mes de agosto del año 2020.

Con lo anterior, se da por concluida la segunda sesión, firmando al calce los intervinientes e integrantes del Comité de Transparencia de la CEMERGE, para los efectos legales a que haya lugar.

---

**LIC. KALEOPPY ORNELAS CÁRDENAS  
DIRECTORA DE MEJORA REGULATORIA Y PRESIDENTE  
DEL COMITÉ DE TRANSPARENCIA**

---

**LIC. PERLA VANESSA ORTÍZ NAVARRETE  
DIRECTORA DE GESTIÓN EMPRESARIAL Y MIEMBRO  
DEL COMITÉ DE TRANSPARENCIA  
(INDISPUESTA PARA FIRMA POR INCAPACIDAD)**

---

**LIC. RUTH AYAME SAITO MURGUIA  
COORDINADORA ADMINISTRATIVA Y MIEMBRO  
DEL COMITÉ DE TRANSPARENCIA**

Esta hoja forma parte del Acta de Segunda Sesión CEMERGE-CT/14082020 del Comité de Transparencia de la Comisión Estatal de Mejora Regulatoria y Gestión Empresarial, para declarar que aprueba el calendario de sesiones ordinarias, así como documento de seguridad en materia de tratamiento de datos personales en posesión de CEMERGE, celebrada en esta ciudad de Culiacán Rosales, Sinaloa, a las 13: 00 horas del día 14 de agosto del año 2020.