PODER JUDICIAL

DEL ESTADO DE COAHUILA DE ZARAGOZA

DOCUMENTO DE SEGURIDAD

PODER JUDICIAL DEL ESTADO DE COAHUILA DE ZARAGOZA

Contenido

I. Introducción.

Para el Poder Judicial del Estado de Coahuila de Zaragoza es de suma importancia garantizar la debida protección de datos personales a los que se les da tratamiento en cada uno de los órganos jurisdiccionales, no jurisdiccionales y administrativos que integran este poder público.

El presente documento de seguridad constituye un instrumento que permite a los sujetos obligados conocer las áreas de oportunidad y las líneas de acción que deben atenderse en relación a los riesgos identificados en materia de seguridad de datos personales, para que de acuerdo a la ley de la materia se cumpla objetivamente con los principios y procedimientos que garanticen el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados, cumpliendo con los deberes que reconoce nuestra legislación.

Es por ello que, en el presente documento se detallan las medidas de seguridad técnicas, físicas y administrativas con las que se cuenta, mismas que deben considerarse a fin de evitar la vulneración a los datos personales que custodia este ente como sujeto obligado.

Lo anterior, con fundamento en el artículo 29 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Coahuila de Zaragoza, publicada en el Periódico Oficial del Gobierno del Estado de Coahuila de Zaragoza el día 21 de julio de 2017.

II. Glosario.

- **Bases de datos:** Conjunto ordenado de datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;
- **Catálogo de bases de datos personales:** Lista detallada del conjunto ordenado de bases datos personales que estén en posesión del responsable, ya sea en formato escrito, impreso, digital, sonoro, visual, electrónico, informático u holográfico, referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;
- **Datos personales:** Cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;
- **Derechos ARCO**: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;
- **Documento de seguridad:** Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;
- **Inventario de datos personales**: Lista ordenada y detallada que posea el responsable o encargado, de cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo, concerniente a una

persona física identificada o identificable;

- **Ley:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Coahuila de Zaragoza;
- **Medidas de seguridad**: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;
- **Medidas de seguridad administrativas**: Políticas, acciones 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;
- **Medidas de seguridad físicas:** Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento;
- **Medidas de seguridad técnicas**: Conjunto de acciones, mecanismos y sistemas de los datos personales y los recursos involucrados en su tratamiento;
- **Cómputo en la nube:** Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;
- **Poder Judicial:** Poder Judicial del Estado de Coahuila de Zaragoza.
- **Titular:** La persona física a quien corresponden los datos personales;
- **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, publicación, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales;

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

1) A continuación, se describen las categorías de datos personales con los que cuenta el Poder Judicial, los cuales se anexan al final de este documento (Anexo 1)

- **Datos de identificación y contacto:** nombre, estado civil, RFC, CURP, lugar de nacimiento, fecha de nacimiento, nacionalidad, domicilio, teléfono particular, teléfono celular, correo electrónico, firma autógrafa, edad, fotografía y referencias personales.
- **Datos sobre características físicas:** color de piel, color de cabello, señas particulares, estatura, peso, cicatrices, tipo de sangre.
- **Datos biométricos:** huella dactilar.
- **Datos laborales:** puesto o cargo que desempeña, domicilio de trabajo, correo electrónico institucional, teléfono institucional, referencias laborales, información generada durante los procedimientos de reclutamiento, selección y contratación y experiencia/capacitación laboral.
- **Datos académicos:** trayectoria educativa, título, cédula profesional, certificados y reconocimientos.
- **Datos migratorios:** entrada al país, salida del país, tiempo de permanencia en el país.
- **Datos patrimoniales y/o financieros:** ingresos, egresos y cuentas bancarias.
- **Datos sobre pasatiempos, entretenimiento y diversión:** pasatiempos, aficiones, deportes que practica y juegos de interés.
- **Datos legales:** situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)
- **Otros datos personales**

- **Datos personales sensibles**
- **Datos sobre la ideología:** posturas religiosas, ideológicas, morales, filosóficas.
- **Datos de salud:** estado de salud físico presente, pasado o futuro y estado de salud mental presente, pasado, o futuro.
- **Datos sobre vida sexual:** preferencias sexuales, prácticas o hábitos sexuales.
- **Datos sobre origen étnico o racial:** pertenencia a un pueblo, etnia o región.
- **Datos personales de naturaleza pública:** Datos que por mandato legal son de acceso público.

2) Personas de quienes se obtienen los datos personales:

a) Personas que laboran en el Poder Judicial.

b) Personas externas que prestan algún servicio para el Poder Judicial.

c) Personas externas que participan en actividades que llevan a cabo por el Poder Judicial (capacitaciones y concursos)

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

3) Nivel de seguridad de los datos personales a los que se les da tratamiento en el Poder Judicial:

Para mayor garantía de seguridad en los datos personales y en las bases de datos personales, físicas o electrónicas, donde se concentran los mismos, las medidas de seguridad que se implementarán corresponden a un nivel de

seguridad **medio**, siempre garantizando la confidencialidad, integridad y disponibilidad de los datos personales, tal y como lo expresa la Ley.

4) Transferencias de los datos personales:

Toda transferencia de datos personales se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 16, 68 y 72 de la Ley.

5) Catálogo de bases de datos personales:

Se anexa catálogo de bases de datos personales con las que cuentan las dependencias que integran el Poder Judicial. Esto coadyuva al ejercicio de los derechos ARCO. (Anexo 2)

IV. Las funciones y obligaciones de las personas que traten datos personales.

Las personas titulares encargadas de tratar datos personales son las siguientes:

- **Consejo de la Judicatura**
- **Tribunal Superior de Justicia**

  Presidencia

  - Presidencia
  - Secretaría Técnica y de Transparencia
  - Auditoría Interna
  - Archivo Judicial General
- **Órganos Jurisdiccionales**
  - Central de Actuarios
    - Central de Actuarios de Saltillo

    - Central de Actuarios de Torreón
- Juzgados por Materia
    - Juzgados Civiles
    - Juzgados Familiares
    - Juzgados Letrados
    - Juzgados Mercantiles
    - Juzgados Mixtos
    - Juzgados Penales
- Pleno
    - Secretaría General del Pleno
- Salas
    - Sala Civil y Familiar
    - Sala Penal
    - Sala Regional
- Tribunal Constitucional
- Tribunales Distritales
    - Primer Tribunal Distrital
    - Segundo Tribunal Distrital
    - Tercer Tribunal Distrital
    - Cuarto Tribunal Distrital
- Tribunales Laborales
    - Tribunal Laboral del Distrito Judicial de Saltillo
    - Tribunal Laboral del Distrito Judicial de Torreón
    - Tribunal Laboral del Distrito Judicial de Monclova
    - Tribunal Laboral del Distrito Judicial de la Región Carbonífera
    - Tribunal Laboral del Distrito Judicial de Río Grande
    - Tribunal Laboral del Distrito Judicial de Acuña

- Órganos Especializados
    - Tribunal de Conciliación y Arbitraje
    - Juzgados Especializados en Violencia Familiar contra las Mujeres
    - Juzgados con Especialización Ambiental

- **Órganos No Jurisdiccionales**
    - Centro de Evaluación Psicosocial
    - Centro de Medios Alternos de Solución de Controversias
    - Instituto de Especialización Judicial
    - Instituto Estatal de Defensoría Pública
    - Oficialía de Partes
    - Visitaduría Judicial General
- **Administrativos**
    - Oficialía Mayor

Las personas que desempeñan los puestos como titulares de los órganos jurisdiccionales, no jurisdiccionales y administrativos de este poder público, tienen como funciones y obligaciones las siguientes:

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

f) Garantizar el cumplimiento de los derechos ARCO a los titulares de los datos personales.

V. Registro de incidencias.

Las incidencias con datos personales que se produzcan vulnerarán la debida protección de los mismos, por lo tanto, es necesario que los titulares de las dependencias que integran el Poder Judicial en donde se de tratamiento a datos personales lleven a cabo un registro de las incidencias que comprometen la seguridad de los datos.

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

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

VI. Identificación y autentificación.

La Dirección de Informática, administrará las bajas y altas de correos electrónicos del personal del Poder Judicial, así como las sesiones en los equipos de cómputo.

La persona encargada del Departamento de Informática asigna usuarios y contraseñas, siendo estas últimas aleatorias y se exige que se modifiquen.

La reserva y confidencialidad de estas contraseñas queda bajo la responsabilidad

de la persona a la que se le asignó la cuenta de usuario.

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

VII. Control de acceso y gestión de soporte.

En todo momento, los titulares de los órganos jurisdiccionales, no jurisdiccionales y administrativos del Poder Judicial que dan tratamiento a datos personales deberán tener un control de acceso a sus bases de datos personales físicas o electrónicas, en el cual establecerán medidas de seguridad que salvaguarden la confidencialidad e integralidad de la información resguardada.

En los periodos establecidos por la normatividad aplicable y de acuerdo a las reglas emitidas por el Consejo de la Judicatura, la información física que contenga datos personales deberá enviarse al Archivo Judicial General, el cual deberá de contar con las instalaciones y protección adecuada para el resguardo de la información.

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

VIII. Análisis de riesgos.

De acuerdo a una matriz de análisis de riesgos de los órganos jurisdiccionales, no jurisdiccionales y administrativos del Poder Judicial (anexo 3) que dan tratamiento a datos personales, se consideran como vulneraciones comunes las siguientes:

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

IX.Análisis de brecha.

Derivado del estudio del cuestionario denominado “Medidas de seguridad existentes VS medidas de seguridad faltantes” (anexo 4,) se aplica el nivel de medidas de seguridad en relación a los datos personales que se manejan.

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

X. El plan de trabajo.

El plan de trabajo para la protección de los datos personales que el Poder Judicial llevará a cabo será establecer líneas de acción en los siguientes rubros:

a) Plan de capacitación: acciones que conformarán la capacitación a través de cursos, talleres, conferencias, congresos, a fin de profesionalizar a los servidores públicos, adquiriendo conocimientos técnicos y prácticos para su actualización en materia de transparencia, acceso a la información pública y protección de datos personales.
b) Medidas de seguridad físicas, administrativas y técnicas: implementar medidas para la debida protección de datos personales.

c) Llevar a cabo visitas de seguimiento y verificación con el fin de corroborar el cumplimiento de las obligaciones en materia de protección de datos personales.

XI. Los mecanismos de monitoreo y revisión de las medidas de seguridad.

Las medidas de seguridad administrativas, físicas y técnicas serán de aplicación a todas las bases de datos personales que manejan las personas a cargo de los órganos jurisdiccionales, no jurisdiccionales y administrativos del Poder Judicial, esto de acuerdo a sus funciones y obligaciones.

XII. Los programas de capacitación y actualización.

En materia de protección de datos personales se programará una vez al año una capacitación, la fecha se designará en el transcurso del mismo, de forma tal que lo permitan las actividades laborales de cada servidor público que integra este Poder Judicial.

Asimismo, el personal en materia de transparencia del Poder Judicial, estará en capacitación constante por medio de cursos y/o talleres presenciales o en línea por parte de las entidades locales o federales, a fin de ofrecer al personal asesoría en la materia.

XIII. Actualización del documento de seguridad.

El presente documento de seguridad se actualizará cuando ocurran los siguientes eventos:

I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;

III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad, e

IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

XIV.Anexos.

PODER JUDICIAL
DEL ESTADO DE COAHUILA DE ZARAGOZA

ANEXO 1
INVENTARIO DE DATOS PERSONALES.

Datos personales recabados	Existente	Necesario	No necesario
Datos de identificación y contacto			
Nombre	X		
Estado Civil			
Registro Federal de Contribuyentes (RFC)	X		
Clave Única de Registro de Población (CURP)			
Lugar de nacimiento	X		
Fecha de nacimiento	X		
Nacionalidad			
Domicilio	X		
Teléfono particular	X		
Teléfono celular	X		
Correo electrónico	X		
Firma autógrafa	X		
Firma electrónica			
Edad			
Fotografía			
Referencias personales			
Datos sobre características físicas			
Color de piel			
Color de cabello			
Señas particulares			
Estatura			
Peso			
Cicatrices			
Tipo de sangre			
Datos biométricos			
Imagen del iris			
Huella dactilar			
Palma de la mano			
Datos laborales			
Puesto o cargo que desempeña			
Domicilio de trabajo			
Correo electrónico institucional			
Teléfono institucional			
Referencias laborales			
Información generada durante los procedimientos de reclutamiento, selección y contratación			
Datos personales recabados	**Existente**	**Necesario**	**No necesario**
Experiencia/Capacitación laboral			
Datos académicos			
Trayectoria educativa			
Títulos			
Cédula profesional			
Certificados			
Reconocimientos			
Datos migratorios			
Entrada al país			
Salida del país			
Tiempo de permanencia en el país			
Calidad migratoria			
Derechos de residencia			
Aseguramiento			
Repatriación			
Datos patrimoniales y/o financieros			
Bienes muebles			
Bienes inmuebles			
Información fiscal			

ANEXO 1
INVENTARIO DE DATOS PERSONALES.

Historial crediticio/Buró de crédito			
Ingresos			
Egresos			
Cuentas bancarias			
Números de tarjetas de crédito			
Información adicional de tarjeta (fecha de vencimiento, códigos de seguridad, datos de banda magnética, pin)			
Seguros			
Afores			
Datos sobre pasatiempos, entretenimiento y diversión			
Pasatiempos			
Aficiones			
Deportes que practica			
Juegos de su interés			
Datos legales			
Situación jurídica de la persona (juicios, amparos, procesos administrativos, entre otros)			
Otros datos personales (mencionar)			
Datos personales recabados	**Existente**	**Necesario**	**No necesario**
Datos personales sensibles			
Datos sobre la ideología			
Posturas religiosas/ ideológicas/morales/ filosóficas			
Pertenencia a un partido/Posturas políticas			
Pertenencia a un sindicato			
Datos de salud			
Estado de salud físico presente, pasado o futuro			
Estado de salud mental presente, pasado o futuro			
Información genética			
Datos sobre vida sexual			
Preferencias sexuales			
Prácticas o hábitos sexuales			
Datos de origen étnico o racial			
Pertenencia a un pueblo, etnia o región			
Otros datos personales (mencionar)			

PODER JUDICIAL
DEL ESTADO DE COAHUILA DE ZARAGOZA

ANEXO 2
CATÁLAGO DE BASES DE DATOS PERSONALES

DEPENDENCIA O ENTIDAD: **PODER JUDICIAL DEL ESTADO DE COAHUILA DE ZARAGOZA**

DOMICILIO: Blvd. Francisco Coss #945. Zona Centro. Saltillo, Coahuila de Zaragoza

DEPENDENCIA	NOMBRE DE LA BASE DE DATOS PERSONALES	CATEGORIA:		FINALIDAD PARA		CARGO DEL ENCARGADO DE LA BASE DE DATOS PERSONALES
		ADMINISTRATIVO	JURÍDICO	LA QUE FUERON RECABADOS LOS DATOS	NORMATIVIDAD QUE LES SEA APLICABLE	
Órganos Jurisdiccionales		x	x	REGISTRO DE INFORMACIÓN	LEY DE LA MATERIA	TITULAR DEL ÁREA
Órganos No Jurisdiccionales		x	x	REGISTRO DE INFORMACIÓN	REGLAMENTO INTERNO	TITULAR DEL ÁREA
Administrativos		x		REGISTRO DE INFORMACIÓN	REGLAMENTO INTERNO	TITULAR DEL ÁREA

PODER JUDICIAL
DEL ESTADO DE COAHUILA DE ZARAGOZA

ANEXO 3
MATRIZ DE ANÁLISIS DE RIESGOS

DEPENDENCIA O ENTIDAD: PODER JUDICIAL DEL ESTADO DE COAHUILA DE ZARAGOZA

MATRIZ DE ANÁLISIS DE RIESGOS						
		ANÁLISIS		EVALUACIÓN		TRATAMIENTO O CONTROL OPERACIONAL
NOMBRE DE BASE DE DATOS PERSONALES	RIESGO	PROBABILIDAD	GRAVEDAD	CALIFICACIÓN	NIVEL DEL RIESGO	

Valor de Gravedad (1-4)				
4	8	12	16	
3	6	9	12	
2	4	6	8	
1	2	3	4	

Nivel del riesgo

ALTO (12-16)
MEDIO (8-9)
BAJO (1-6)

PODER JUDICIAL
DEL ESTADO DE COAHUILA DE ZARAGOZA

ANEXO 4
ANÁLISIS DE BRECHA

Análisis de Brecha			
Órganos jurisdiccionales, no jurisdiccionales y administrativos del Poder Judicial.			
Medidas de seguridad existentes VS medidas de seguridad faltantes			
Pregunta o Control	**¿Existente?**		
	SI	**NO**	**Observaciones**
Medidas de seguridad basadas en la cultura del personal			
¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?			
Política de escritorio limpio			
Hábitos de cierre y resguardo			
Impresoras, escáneres, copiadoras y buzones limpios			
¿Tienes mecanismos para eliminar de manera segura la información?			
Destrucción segura de documentos			
Eliminación segura de información en equipo de cómputo y medios de almacenamiento electrónico			
Fijar periodos de retención y destrucción de información			
Tomar precauciones con los procedimientos de re-utilización			
Informar al personal sobre sus deberes mínimos de seguridad y protección de datos			
Fomentar la cultura de la seguridad de la información			
Difundir noticias en temas de seguridad			
Asegurar la protección de datos personales en subcontrataciones			
¿Tienes procedimientos para actuar ante vulneraciones a la seguridad de los datos personales?			
Tener un procedimiento de notificación			
¿Realizas respaldos periódicos de los datos personales?			
Medidas de seguridad en el entorno de trabajo físico			
¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?			
Mantener registros del personal con acceso al entorno de trabajo			

ANEXO 4
ANÁLISIS DE BRECHA

Análisis de Brecha			
(Medidas de seguridad existentes VS medidas de seguridad faltantes)			
Pregunta o Control	¿Existente?		
	SI	NO	Observaciones
¿Tienes medidas de seguridad para evitar el robo?			
Cerraduras y candados			
Elementos disuasorios			
¿Cuidas el movimiento de información en entornos de trabajo físicos?			
Aprobación de salida de documentos, equipo de cómputo y/o medios de almacenamiento electrónico			
Mantener en movimiento sólo copias de la información, no el elemento original			
Usar mensajería certificada			
Medidas de seguridad en el entorno de trabajo digital			
¿Realizas actualizaciones al equipo de cómputo?			
¿Revisas periódicamente el software instalado en el equipo de cómputo?			
¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?			
Uso de contraseñas y/o cifrado			
Bloqueo y cierre de sesiones			
Administrar usuarios y accesos			
¿Revisas la configuración de seguridad del equipo de cómputo?			
¿Tienes medidas de seguridad para navegar en entornos digitales?			
Reglas de navegación segura			
Uso de conexiones seguras			
¿Cuidas el movimiento de información en entornos de trabajo digitales?			
Seguridad de la información enviada y recibida			