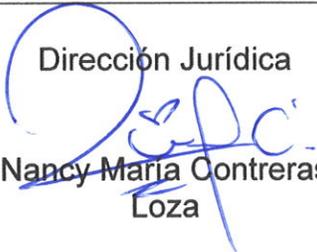
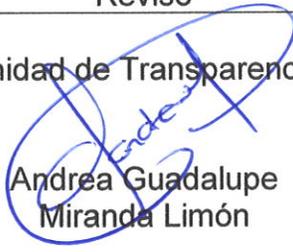
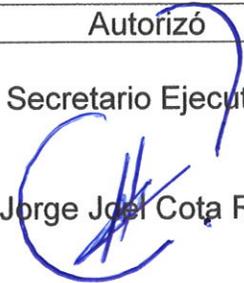




## Documento de Seguridad de Datos Personales Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal

Elaboró	Revisó	Autorizó
Dirección Jurídica  Nancy María Contreras Loza	Unidad de Transparencia  Andrea Guadalupe Miranda Limón	Secretario Ejecutivo  Jorge Joel Cota Ruíz

La Paz, Baja California Sur, a noviembre de 2023.



## ÍNDICE

1. Presentación.....	3
2. Objetivo y alcance del documento.....	5
3. Sistema de gestión de los datos personales en posesión de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal.....	5
4. Inventario de Datos Personales de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur.....	10
5. Análisis de riesgos y de brecha.....	13
5.1 Elementos para el análisis de riesgos .....	13
5.2 Estado actual del riesgo de datos personales .....	15
6. Medidas de seguridad generales.....	16
6.1 Monitoreo de las medidas de seguridad.....	20
7. Propuesta de capacitación en materia de datos personales.....	21
8. Funciones y responsabilidades del tratamiento de datos personales.....	22
9. Programa de trabajo para la implementación de medidas de seguridad.....	26



## 1. Presentación.

La Constitución Política de los Estados Unidos Mexicanos en los artículos 6 y 16 incorpora el derecho de toda persona a la protección de sus datos personales, así como al acceso, rectificación, cancelación y oposición en los términos que determina la Ley.

La Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur (LPDPPSOBCS) establece por su parte un conjunto de bases, principios y procedimientos para garantizar el derecho a la protección de datos con carácter personal y que se encuentren en posesión de los sujetos obligados, entre los que figura la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur (SECESSJP).

De ahí que el presente Documento de Seguridad tiene como propósito establecer el marco de referencia del tratamiento de los datos personales que se llevan a cabo al interior de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, por las diversas unidades administrativas que conforman su estructura orgánica, a fin de mantener vigente y promover la mejora continua en la protección de los mismos, en términos de lo previsto en los artículos 29 y 30 de la LPDPPSOBCS, además de desarrollar buenas prácticas en la materia.

En ese sentido, la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para Estado de Baja California Sur, ha identificado los procesos que en el ámbito de su competencia involucran el tratamiento de datos personales, a efecto de mantener la seguridad de los mismos durante el ciclo de vida de la información, indicando la forma en la que se trata, las medidas de seguridad adoptadas y las áreas responsables de su protección, así como las finalidades del tratamiento de acuerdo a sus respectivos ámbitos de funciones.

Considerando que los datos personales constituyen el principal activo de información objeto del presente documento, es necesario señalar que todos y cada uno de los elementos que lo integran, constituyen un sistema interno para la gestión y tratamiento de los datos personales en posesión de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, pues tal y como lo dispone el artículo 29 de la LPDPPSOBCS, se entiende por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales.



Así, la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, comprometida con la tutela de los datos personales que trata, ha impulsado a su interior las acciones conducentes para evitar la alteración, pérdida, transmisión y acceso no autorizados a los datos, mediante la implementación de medidas físicas, administrativas y técnicas, tendentes a garantizar la seguridad e integralidad de los mismos, así como su seguimiento y supervisión continuos.

De ahí, que dicho Sistema permita disponer de información relacionada con las medidas de seguridad, el análisis general de las amenazas y posibles vulnerabilidades, así como los mecanismos o acciones a implementar para mitigarlas.

El presente documento se integra a partir la gestión de actividades coordinadas para controlar y verificar que el tratamiento de los datos personales sea acorde con los principios que rigen su protección, pues para la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, la política de seguridad en esta materia constituye un compromiso con el cumplimiento de las disposiciones previstas en la citada LPDPPSOBCS.

Para ello, en términos de lo previsto en el artículo 31, fracción II de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur, el cual establece que el responsable deberá mantener actualizado su documento de seguridad como resultado del proceso de mejora continua, la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, llevó a cabo un inventario de datos personales; establecimiento de las medidas de seguridad adoptadas con motivo de su tratamiento y, el análisis de riesgo y brecha, con el objeto de monitorear las medidas adoptadas, identificar posibles vulneraciones y mitigar los riesgos; además de avanzar en un proceso de sensibilización permanente respecto de la relevancia que tiene para la institución las medidas correctivas y preventivas, en función de los resultados obtenidos de la revisión de los sistemas de datos, acorde a los esquemas de autorregulación y capacitación del personal.



## **2. Objetivo y alcance del documento.**

Establecer los principales elementos que integran las medidas de seguridad administrativas, físicas y técnicas que ha adoptado la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, para garantizar la confidencialidad, integridad y disponibilidad de los datos personales; así como determinar las posibles vulnerabilidades, amenazas y riesgos de los que pueden ser objeto en un plano general los diversos sistemas de información y procesos en los se tratan datos personales por las diversas unidades administrativas, conforme a lo establecido en la LPDPPSOBCS.

El alcance de este documento se relaciona con la identificación de sistemas de información o procesos administrados por parte de las Direcciones que conforman la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, a saber: Dirección Jurídica y Dirección Administrativa, en los que, de acuerdo con su ámbito de funciones llevan a cabo el uso y tratamiento de datos personales, mismos que se encuentran bajo su estricta responsabilidad tanto en los medios electrónicos como en los espacios físicos en que se administran, operan y resguardan dichos datos personales.

En este sentido, la Unidad de Transparencia integra el presente documento de seguridad con base en la información generada por las citadas unidades administrativas acorde al ámbito de sus funciones y, de conformidad con las disposiciones aplicables.

## **3. Sistema de gestión de los datos personales en posesión de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal**

Para el tratamiento de los datos personales que lleva a cabo la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, a través de su obtención, uso, registro, conservación, acceso, manejo, aprovechamiento, transferencia, disposición o cualquier otra operación aplicable a los mismo, se realiza el establecimiento de políticas y métodos orientados a salvaguardar su confidencialidad, integridad y disponibilidad, conforme a los preceptos previstos por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur y la Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur



En tal virtud, la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, inició su proceso de planificación de los esquemas de protección de datos mediante la identificación de todos y cada uno de los procesos y tareas en los que, de acuerdo con el ámbito de funciones de las distintas áreas que conforman la institución, se involucra el tratamiento de datos personales considerando los elementos mínimos que establece el artículo 28, fracción II de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur.

Es así que a través del desarrollo que, se llevó a cabo el levantamiento del inventario de datos, con el propósito de identificar, entre otros aspectos, la categoría y tipo de datos que son sometidos a tratamiento, incluyendo los de carácter sensible; los Medios a través de los cuales se obtienen dichos datos; el sistema físico y/o electrónico que se utiliza para su acceso, manejo, aprovechamiento, monitoreo y procesamiento; las características del lugar donde se ubican las bases físicas o electrónicas de datos; las finalidades del tratamiento, y el nombre, cargo y adscripción de las personas servidoras públicas que tienen acceso al tratamiento.

De igual forma, una vez integrados los inventarios de datos, se dispuso de la metodología para la elaboración del análisis de riesgos, en la cual, atendiendo a lo previsto en el artículo 28, fracción IV de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur, las áreas responsables de su tratamiento identificaron el valor de los datos personales de acuerdo con su categoría y el ciclo de vida; el valor de exposición de los activos involucrados en el tratamiento; las consecuencias que pueden generarse para los titulares de los mismos con motivo de su posible vulneración y los factores de riesgo a los que eventualmente se encuentran expuestos.

Con base en dicho análisis de riesgo, además de promover el reconocimiento de las medidas de seguridad administrativas, entendidas como el conjunto de políticas y procedimientos de gestión, soporte y revisión de la seguridad de la información; físicas, que corresponden a las acciones o mecanismos para proteger el entorno físico de los datos, así como de los recursos involucrados en su tratamiento y, técnicas que se valen de la tecnología para proteger el entorno digital de la información, también se han registrado nuevas medidas de seguridad que deberán desarrollarse para fortalecer algunos de los controles que actualmente son implementados; es decir, el análisis de brecha a partir del cual será posible mitigar los riesgos a los que están expuestos los datos tratados.



Considerando que la identificación de vulnerabilidades tiene por objeto prevenir posibles dificultades en la seguridad de los datos bajo un enfoque proactivo; es decir, identificar áreas de oportunidad en materia de seguridad de datos personales sin que éstas constituyan un daño efectivo, es que se listan como posibles vulnerabilidades, las siguientes:

1. Controles de acceso físico y electrónicos inadecuados a sistemas de archivos.
2. Deficiente conocimiento de procedimientos en materia de seguridad de datos.
3. Inadecuada administración de autorizaciones de accesos a los datos personales (sistemas de privilegio).
4. Falta de definición de perfiles y roles para delimitar funciones manejo y uso de datos.
5. Falta de seguimiento y monitoreo a políticas de seguridad.
6. Ausencia de mecanismos de confidencialidad por parte del personal (interno) o por terceros (externos).

Aunado a las anteriores vulnerabilidades, de manera enunciativa más no limitativa, se examinan algunos tipos de amenazas, que pueden ser intencionales o no, a las que podría enfrentarse la institución y sus activos de información.

#### **TIPOS DE AMENAZAS**

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizada.
- Pérdida o destrucción no autorizada.

El riesgo que de manera general puede presentarse en caso de que las amenazas señaladas exploten las vulnerabilidades, es el de facilitar el acceso a los datos personales de manera no autorizada con el fin de comprometer su confidencialidad, disponibilidad e integridad, por lo que las medidas de seguridad por parte de las áreas están orientadas a proteger los datos personales.



A partir de la identificación de vulnerabilidades y amenazas, se han establecido medidas de seguridad generales, que de acuerdo a la experiencia y mejores prácticas son monitoreadas para lograr la mejora continua por parte de todos los involucrados en el tratamiento. Como parte del sistema de gestión y política de seguridad institucional se enmarcan las reglas generales siguientes:

- A. Tratar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur;
- B. Sujetar el tratamiento de los datos personales al principio de consentimiento, salvo las excepciones previstas por la Ley;
- C. Informar a los titulares del tratamiento de los datos y sus finalidades;
- D. Procurar que los datos personales tratados sean correctos y estén actualizados.
- E. Suprimir los datos personales cuando hayan dejado de ser necesarios para las finalidades para las cuales se obtuvieron.
- F. Tratar los datos personales estrictamente para propósitos legales o legítimos de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur;
- G. Limitar el tratamiento de los datos personales al cumplimiento de las finalidades;
- H. No obtener datos personales a través de medios fraudulentos;



- I. Respetar la expectativa razonable de privacidad del titular;
- J. Tratar estrictamente los datos personales necesarios, adecuados y relevantes en relación con las finalidades;
- K. Velar por el cumplimiento de los principios;
- L. Establecer y mantener medidas de seguridad;
- M. Guardar la confidencialidad de los datos personales;
- N. Identificar el flujo y ciclo de vida de los datos personales;
- O. Mantener actualizado el inventario de datos personales o de las categorías que maneja la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur;
- P. Respetar los derechos de los titulares en relación con sus datos personales;
- Q. Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales; y,
- R. Identificar a las personas servidoras públicas de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, responsables del tratamiento de los datos personales.



Con base en lo anterior, la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur determina las pautas de acción del personal encargado de tratamiento de datos personales con miras a generar su correcto resguardo, buscando en todo momento actuar en apego a las directrices de la LPDPPSOBCS.

#### **4. Inventario de Datos Personales de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur.**

Para cumplir con los objetivos y obligaciones que prevé la LPDPPSOBCS, particularmente en materia de seguridad y, como parte del Sistema de Gestión de Seguridad de Datos Personales de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, se realizó una revisión dentro las unidades administrativas que conforman su estructura orgánica, para identificar los procesos prioritarios en los que actualmente se lleva a cabo tratamiento de datos personales; obteniendo con ello el denominado Inventario de Datos Personales de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur.

Por inventario de tratamiento de datos, se entiende el control documentado del conjunto de operaciones que realizan las áreas que integran la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, con motivo de los datos que se recaban de las personas, a través de procedimientos automatizados o físicos, que van desde su obtención, registro, organización, conservación, utilización, cesión, difusión, interconexión, hasta la rectificación, cancelación y oposición, con motivo de la atención del ejercicio de éstos derechos en el ámbito de sus atribuciones.

En tal virtud, en coordinación con las áreas y derivado del proceso de actualización de información, se advirtió que, en general 2 de las 2 unidades administrativas que conforman la estructura orgánica de la institución llevan a cabo el tratamiento de datos personales.



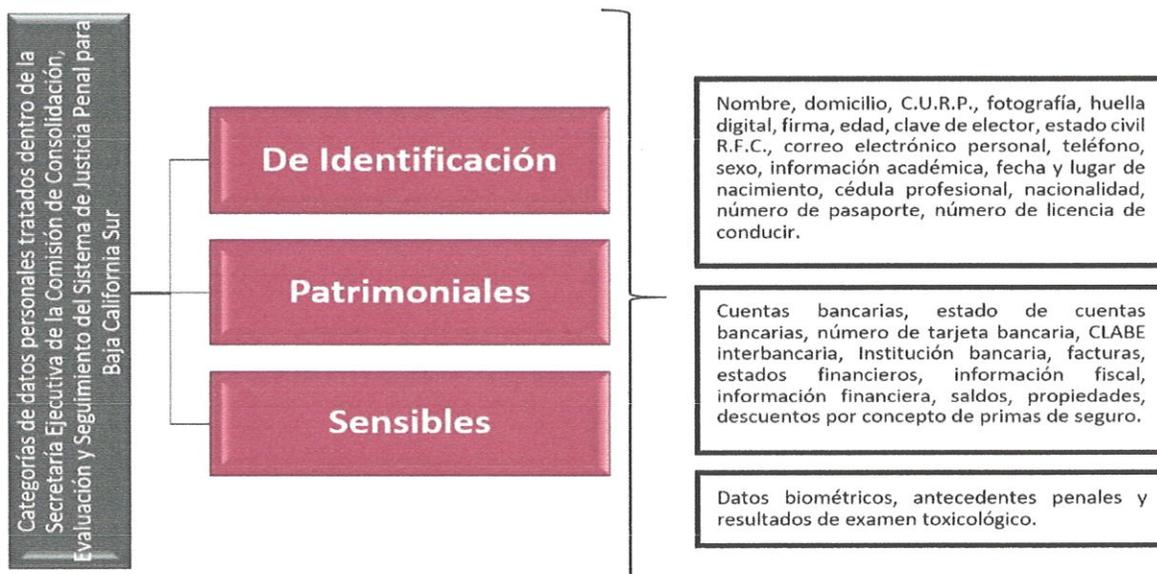
## Estructura Orgánica de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur

- Dirección Jurídica.
- Dirección Administrativa.

Se advirtió que en las 2 unidades administrativas en la que se tratan datos, a través una o varias de las áreas que las conforman, dicho tratamiento atiende a las operaciones o procesos que realizan con motivo del ejercicio de sus facultades.

La Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, lleva a cabo diversos procesos dentro de las unidades administrativas, cuyas actividades involucran tratamientos de datos incluyendo las actividades de carácter administrativo derivadas de recursos humanos, materiales y financieros, los procesos de capacitación, así como el cumplimiento a las obligaciones en materia de transparencia, dada su calidad de sujeto obligado en materia de datos personales.

Asimismo, durante el proceso de sistematización se observó que los datos personales cuyo tratamiento se lleva a cabo en los 5 procesos identificados, corresponden a las siguientes 3 categorías:





A partir de lo anterior, el Inventario de Datos Personales de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, realizó la identificación de las áreas con mayor incidencia en el tratamiento de datos personales, a fin de enfocar los trabajos de atención para el cumplimiento de las disposiciones jurídicas en materia de protección de datos.

Sobre el particular, se identificó que por lo que hace al tratamiento de datos de identificación, en las 2 unidades administrativas se llevan a cabo tratamientos de datos de esta naturaleza; respecto a los patrimoniales en 1 de ellas se realiza tratamiento de éstos, y en Relación a los sensibles, en 1 unidades administrativas tratan este tipo de datos.

Lo anterior permite advertir que la categoría de datos personales con mayor número de áreas y procesos son los de carácter identificativos, seguidos por los patrimoniales.

A partir de lo anterior, se puede advertir que tanto la Dirección Administrativa como la Dirección Jurídica cuentan con procesos en los que se tratan datos personales.

Como se puede observar, la Dirección Jurídica posee el mayor número de operaciones en las que intervienen tratamientos de datos personales, por tal motivo, las áreas de atención, oportunidad y verificación en materia de protección de datos deben contar con un enfoque de importancia en el desarrollo de las actividades de esta unidad administrativa.

Ante este contexto, es posible concluir que el Inventario de Datos Personales de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, a partir de la identificación de las áreas con mayor incidencia en su tratamiento, se constituye como un elemento del Sistema de Gestión de Datos Personales, que junto con las medidas de seguridad representa un instrumento de evidencia para la implementación de las directrices de la Política en materia de protección de datos personales. Asimismo, establece las necesidades de realizar capacitación focalizada en materia de protección de datos para fortalecer la estructura de los operadores en cada uno de los procesos en que se tratan datos, buscando con ello sensibilizar y preparar a los responsables y encargados de los mismos.



En tal virtud, el Inventario de Datos Personales de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, se inscribe como un elemento más de la política para el cumplimiento de las directrices determinadas por la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Baja California Sur, aportando con ello certeza a la ciudadanía de cuáles son y cuál es el destino de los datos recabados.

## **5. Análisis de riesgos y de brecha.**

El presente análisis identifica el riesgo inherente a los datos personales en el tratamiento que reciben por la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, al ejercer sus atribuciones, de manera que pueda ser controlado por la institución para satisfacer el derecho humano a la autodeterminación informativa.

La LPDPPSOBCS en sus artículos 27, fracción I, y 28, fracción IV, considera que el determinar el riesgo inherente a los datos personales tratados es un deber de los sujetos obligados en la adopción de medidas de seguridad, para lo que deben realizar un análisis que considere las amenazas y vulnerabilidades para los datos, así como los recursos involucrados en el tratamiento.

Con base en la LPDPPSOBCS, la valoración de los riesgos de los datos personales forma parte de los elementos mínimos que debe contener el instrumento que describe y da cuenta, en lo general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas (Documento de seguridad), en este caso, por la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos bajo su posesión.

### **5.1 Elementos para el análisis de riesgos**

La seguridad de los datos personales que se tratan en la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, demanda conocer y entender los riesgos a los que se encuentran expuestos en los distintos procesos que realizan las unidades administrativas, lo que permitiría afrontarlos de manera adecuada y oportuna.



Para analizar los riesgos de los datos personales que son objeto de tratamiento por la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, se elaboró un instrumento que, a partir de considerar su objeto y atribuciones constitucionales, clasifica los datos en tres tipos, tal y como ha sido referenciado con antelación.

- 1) De identificación o contacto, que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la edad.
- 2) Patrimoniales, que comprenden la información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.
- 3) Sensibles, que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como, por ejemplo, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

Para la determinación del riesgo sobre esa tipología de datos personales se valora la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión y eliminación (ciclo de vida), en correspondencia con una diversidad de activos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza). Para facilitar el análisis, se establecieron cuatro tipos de amenazas:

- Robo, extravío o copia no autorizada.
- Uso, acceso o tratamiento no autorizado.
- Daño, alteración o modificación no autorizada.
- Pérdida o destrucción no autorizada.

Esto es, se tomó en cuenta la probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida de los datos personales. Así, se consideró la consecuencia desfavorable leve, moderada o grave en caso de que la amenaza ocurra (impacto).



La identificación y valoración del riesgo en cada proceso en que se tratan datos personales por las unidades administrativas de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, se basaron en una escala del 0 al 3, representándose de la forma siguiente:

Rango	Valor del Riesgo
Cuando el valor es $\leq 1$	Bajo
Cuando $> 1$ y $< 2$	Medio
Cuando el valor es $\geq 2$	Alto

## 5.2 Estado actual del riesgo de datos personales

En general se tiene que la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, cuenta con 2 unidades administrativas de nivel Dirección, en las que se da tratamiento de datos personales mediante 5 procesos prioritarios.

El promedio de riesgo que se presenta en el conjunto de procesos de los que es responsable cada una de las 2 unidades administrativas que trata datos personales en la SECESSJP, se ubican en la misma posición la Dirección Administrativa y la Dirección Jurídica con 1.0.

Al considerar el ciclo de vida de los datos personales (obtención, tratamiento, almacenamiento, transferencia o remisión y eliminación), mediante el análisis de riesgos fue posible identificar la frecuencia con que se atribuye la actualización de riesgos en cada etapa, donde destaca la transferencia con el porcentaje más alto: 30%, mientras que el bloqueo recibe el mínimo porcentaje: 20%.

En la etapa de obtención de datos personales, la amenaza que se presenta con mayor frecuencia es la de Robo, extravío o copia no autorizada, con un 30% de los casos; seguida de Pérdida o destrucción no autorizada, con 25%; Uso, acceso o tratamiento no autorizado, con 25%, y por último Daño, alteración o modificación no autorizado, con 20%.

En el almacenamiento de datos personales, la amenaza más frecuente es el Daño, alteración o modificación no autorizado, con 29%, el Robo, extravío o copia no autorizada, con 26%; después la Pérdida o destrucción no autorizada, con 25%; y el Uso, acceso o tratamiento no autorizado, con 20%.



En la etapa de tratamiento de datos personales, la amenaza identificada con mayor peso es la Pérdida o destrucción no autorizada, con 25%; enseguida se encuentran con el mismo porcentaje el Robo, extravío o copia no autorizada, con 25% así como el Daño, alteración o modificación no autorizado, con 25% y por último el Uso, acceso o tratamiento no autorizado, que alcanza un 25%.

En la transferencia de datos personales, la amenaza más alta es el Uso, acceso o tratamiento no autorizado, con 30%; seguida del Daño, alteración o modificación no autorizado, con 25%, Robo, extravío o copia no autorizada, con 23%; y con menos porcentaje la Pérdida o destrucción no autorizada, con 22%.

En la etapa de eliminación de datos personales, la distribución de las amenazas fue uniforme para los cuatro supuestos de estas: Robo, extravío o copia no autorizada con 25%; Uso, acceso o tratamiento no autorizado con 25%; Daño, alteración o modificación no autorizado con 25%; y Pérdida o destrucción no autorizada con 25%.

Con base en el promedio de riesgo identificado en las distintas unidades administrativas que tratan datos personales, así como el detectado en cada etapa del ciclo de vida de esos datos, se tiene que, de manera general, en la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, el nivel de riesgo bajo es el que predomina.

## **6. Medidas de seguridad generales.**

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta la SECESSJP para mantener la confidencialidad e integralidad de la información, así como para proteger los datos personales contra daño, pérdida, destrucción o alteración, así como evitar el uso, acceso o tratamiento no autorizado, e impedir la divulgación no autorizada, son las siguientes:

### **A. Medidas administrativas.**

1. Adopción de un esquema de capacitación permanente en materia de la Ley de Protección de Datos Personales en posesión de Sujetos Obligados para el Estado de Baja California Sur (LPDPPSOBCS), impartido mediante por el organismo garante.



2. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.
3. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes técnicos.
4. Mecanismos de control desarrollados conforme a lo establecido en los lineamientos del Sistema de Gestión de Documentos institucional.
5. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
6. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

#### **B. Medidas físicas.**

1. Resguardo de documentos e información en archivos físicos de trámite y concentración.
2. Disponer de la instalación de chapas con llave para mantener control de acceso de personas a espacios de resguardo de información.
3. Limitar el número de personas con acceso a archivos físicos.
4. Realizar el registro de personas con acceso a espacios físicos en los que se resguarda información con datos personales.
5. Procurar suscribir responsivas de confidencialidad con el personal que trata datos personales.



6. Designación de personal con acceso controlado a espacios de resguardo físico de expedientes y documentos con datos personales.
7. Resguardo de llaves en oficinas de acceso restringido.

### **C. Medidas técnicas.**

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registrarlas a la vista de otras personas.
2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.
3. Notificar de manera inmediata al Departamento de Informática los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.
4. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.
5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.
6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.



7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.
8. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.
9. Borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que nos son necesarios para el desarrollo de funciones.
10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado.

Adicionalmente, como parte de la política de seguridad técnica, la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur implementa los siguientes controles:

1. Definición de políticas de contraseñas.
2. Asignación de privilegios de acuerdo a roles y funciones.
3. Autenticación de correo electrónico.
4. Acceso a los sistemas conforme a procedimiento de administración de usuarios y contraseñas con cuenta local con permiso de administrador.
5. Borrado seguro de la información que reside en los equipos de cómputo.
6. Deshabilitación de cuentas de personal que causa baja.
7. Acceso controlado de administración, accesos privilegiados y seguridad de la información.



### **6.1 Monitoreo de las medidas de seguridad.**

1. La supervisión de las medidas de seguridad técnicas y físicas es un elemento importante para la mejora continua, pues permite definir nuevos controles de monitoreo y seguimiento de éstas. Entre las medidas de supervisión y monitoreo se encuentran las siguientes:
2. Revisar la actualización permanente del esquema de contraseñas conforme a las pantallas de parametrización de los sistemas, verificando que los valores se encuentren determinados conforme a la política.
3. Monitorear que todas las cuentas que se dan de alta para otorgar acceso a la red, sea validada en el campo correspondiente a la contraseña, a fin de asegurar el uso.
4. Revisar el cumplimiento de protocolos.
5. Validar que los accesos, baja o cambio a sistemas se realicen conforme al proceso de administración de usuarios.
6. Vigilar que el ingreso de personas sea a través de los accesos correspondientes, plenamente identificados.



## **7. Propuesta de capacitación en materia de datos personales.**

Uno de los factores esenciales para la implementación de los controles y demás medidas de seguridad, la actualización y mejora continua del inventario de datos personales, el apego a la normatividad y a Ley, así como la concientización en la materia por parte del personal involucrado en el tratamiento de datos personales, es el conocimiento y capacitación, por lo que, el aprovechamiento de los recursos y herramientas que el propio Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Baja California Sur (ITAI) ha dispuesto para su uso y obtención de beneficios, se propone que a través del Instituto de Capacitación para los Trabajadores del Estado de Baja California Sur (ICATEBCS), se desarrolle un programa de capacitación focalizada, mediante el cual profundice en el conocimiento de la materia por parte de los servidores públicos que intervienen en el tratamiento de datos personales.

Así, entre los elementos de los que resulta necesario profundizar se encuentran los siguientes:

- I. Introducción al derecho a la protección de datos personales.
  - Principios.
  - Deberes.
  - Sistemas de datos personales.
  - Medidas de seguridad.
  - Procedimientos y sanciones/ Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).
  - Medios de defensa.
  
- II. La LPDPPSOBCS.
  - Antecedentes.
  - ¿A quién aplica?
  - ¿Qué objeto tiene?



III) Fundamentos conceptuales de la LPDPPSOBCS.

- Inventario y Base de Datos.
- Medidas de seguridad.
- Análisis de brecha y de riesgo.
- Funciones y obligaciones.

IV) Relevancia de los Avisos de Privacidad.

- Consentimiento.
- Deber de información.
- Finalidades del tratamiento de los datos.

**8. Funciones y responsabilidades del tratamiento de datos personales.**

A raíz de los procesos determinados en el Inventario de Datos Personales, por las áreas que integran las unidades administrativas que realizan tratamiento de éstos dentro de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal para el Estado de Baja California Sur, resultó necesario asociar dichas actividades con las facultades que el Reglamento Interior otorga a las personas servidoras públicas responsables de dicho tratamiento, a efecto de generar certeza y dar cumplimiento al principio de legalidad que debe atender todo servidor público.



En tal virtud, a continuación, se precisan las funciones otorgadas por el ordenamiento jurídico a las personas servidoras públicas que llevan a cabo tratamiento de datos personales dentro de las unidades administrativas que conforman la estructura orgánica de esta institución:

Unidad Responsable	Nombre y Cargo del personal responsable del tratamiento de datos	Funciones relacionadas con el tratamiento de datos	Obligaciones
Dirección Administrativa	Concepción Magallanes Cienfuegos	<p>Artículo 11 del Reglamento Interior de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal (Pendiente de publicar).</p> <p>V. Administrar y optimizar los recursos humanos, materiales y financieros asignados a la Secretaría Ejecutiva;</p> <p>XI. Verificar la correcta integración de los archivos del personal, inventario de bienes y los contratos de adquisiciones, arrendamientos y prestación de servicios;</p> <p>XII. Coordinar, y tramitar los movimientos del personal de altas y bajas, así como las incidencias que se presenten, integrando el registro del personal correspondiente, de conformidad con la normatividad aplicable;</p>	Recepción, registro y resguardo de datos personales.



<p>Dirección Administrativa</p>	<p>Concepción Magallanes Cienfuegos</p>	<p>Artículo 11 del Reglamento Interior de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal (Pendiente de publicar).</p> <p>XIII. Establecer la coordinación para la oportuna programación de los procesos de adquisición, licitación o adjudicación de bienes muebles, inmuebles, servicios u obras relacionados con las funciones de la Secretaría Ejecutiva;</p> <p>XV. Realizar las gestiones y trámites correspondientes para la ejecución presupuestaria de la Secretaría Ejecutiva, previa autorización de la persona titular de la Secretaría Ejecutiva;</p>	<p>Recepción, registro y resguardo de datos personales.</p>
<p>Dirección Jurídica</p>	<p>Nancy María Contreras Loza</p>	<p>Artículo 17 del Reglamento Interior de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal (Pendiente de publicar).</p> <p>VIII. Llevar el registro y resguardo de convenios, acuerdos y demás actos jurídicos en los que intervenga la Secretaría Ejecutiva;</p>	<p>Recepción, registro y resguardo de datos personales.</p>



Dirección Jurídica	Nancy María Contreras Loza	<p>Artículo 17 del Reglamento Interior de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal (Pendiente de publicar).</p> <p>XII. Elaborar estudios estadísticos que proporcionen elementos para la toma de decisiones del Sistema de Justicia Penal en el Estado;</p>	Recepción, registro y resguardo de datos personales.
Dirección Jurídica	Nancy María Contreras Loza	<p>Artículo 17 del Reglamento Interior de la Secretaría Ejecutiva de la Comisión de Consolidación, Evaluación y Seguimiento del Sistema de Justicia Penal (Pendiente de publicar).</p> <p>XIII. Dirigir las acciones encaminadas a la promoción y ejecución de cursos, diplomados, talleres, conferencias, seminarios, capacitaciones y/o especializaciones locales y foráneos, competencia de la Secretaría Ejecutiva;</p>	Recepción, registro y resguardo de datos personales.



## **9. Programa de trabajo para la implementación de medidas de seguridad.**

Conforme al análisis de brecha, existen algunas medidas de seguridad que se requieren implementar, por lo que a continuación se presentan las actividades generales que se planean realizar:

- Celebración de reuniones de trabajo con unidades administrativas, a efecto identificar alternativas de solución técnicas, físicas y administrativas a desarrollar en el mediano y largo plazo.
- Implementar mecanismos de divulgación y conocimiento de las políticas generales de seguridad y, verificar de manera continua su cumplimiento.
- Fortalecer los mecanismos de control de documentos e información en las distintas unidades administrativas, a efecto de evitar posibles vulneraciones.