# Documento de Seguridad de Datos Personales

# Contraloría General

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

# Documento de Seguridad de Datos Personales

# Contraloría General

| Elaboró: | Revisó: | Autorizó: |
|---|---|---|
| Departamento Administrativo y de Acceso a la Información Pública | Unidad de Transparencia de la Contraloría General | Contralora General |
| María José Peralta | Mónica Aguirre Rosales | Rosa Cristina Buendia Soto |

## Índice

## 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 Contraloría General del Estado de Baja California Sur (CG).

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 Contraloría General del 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 Contraloría General del 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 Contraloría General del 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 Contraloría General del 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 Contraloría General del 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 Contraloría General del 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 adoptar medidas correctivas y preventivas, en función de los resultados obtenidos de la revisión de los sistemas de datos, a la luz 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 Contraloría General del 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 Contraloría General del Estado de Baja California Sur, a saber: Dirección de Control de Obras, Dirección de Auditoría Gubernamental, Dirección de Seguimiento a Programas Federales, 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 Contraloría General del Estado de Baja California Sur.

Para el tratamiento de los datos personales que lleva a cabo la Contraloría General del 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 Contraloría General del 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 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 los servidores públicos 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 autorizado.
- Pérdida o destrucción no autorizada.
- Otras.

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 Contraloría General del 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 Contraloría General del 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 los servidores públicos de la Contraloría General del Estado de Baja

California Sur, responsables del tratamiento de los datos personales.

Con base en lo anterior, la Contraloría General del 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 Contraloría General del 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 Contraloría General del Estado de Baja California Sur, se realizó una revisión dentro las unidades administrativas que conforman su estructura orgánica, para identificar los procesos pripritarios en los que actualmente se lleva a cabo tratamiento de datos personales; obteniendo con ello el denominado Inventario de Datos Personales de la Contraloría General del 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 Contraloría General del 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 6 de las 6 unidades administrativas que conforman la estructura orgánica de la institución llevan a cabo el tratamiento de datos personales.

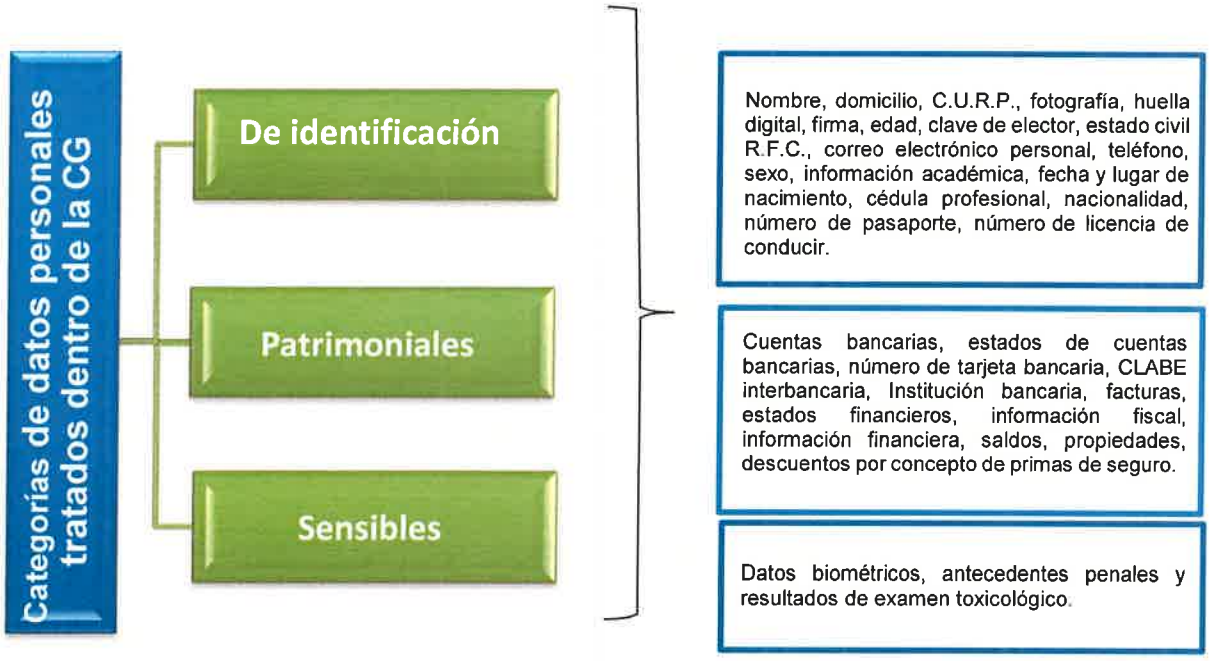
**Estructura Orgánica de la Contraloría General del Estado de Baja California Sur**

1. Dirección de Control de Obras.
2. Dirección de Auditoría Gubernamental.
3. Dirección Jurídica.
4. Dirección Administrativa.
5. Dirección de Seguimiento a Programas Federales.
6. Dirección de Anticorrupción.

Se advirtió que en las 6 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 Contraloría General del Estado de Baja California Sur, lleva a cabo diversos procesos dentro de las unidades administrativas, cuyas actividades involucran tratamientos de datos debido a la fiscalización e investigación que llevan a cabo, sin embargo, también determina operaciones de naturaleza jurídica y administrativa que no derivan, necesariamente, del proceso de fiscalización, pero que sí permiten generar las condiciones para un desarrollo óptimo de sus atribuciones de auditoría. Ejemplo de ello son 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 13 procesos identificados, corresponden a las siguientes 3 categorías:



A partir de lo anterior, el Inventario de Datos Personales de la Contraloría General del Estado de Baja California Sur, posibilitó la identificación de hallazgos en relación con el tratamiento de datos personales, aportando los elementos que permiten focalizar las áreas con mayor incidencia en el tratamiento de éstos, y con ello, 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 6 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 **6** 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 y sensibles**, seguidos por los patrimoniales.

A partir de lo anterior, también se puede advertir que la unidad administrativa con procesos en los que se tratan datos personales es la Dirección Jurídica, seguida por la Dirección Administrativa.

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 dable concluir que el Inventario de Datos Personales de la Contraloría General del Estado de Baja California Sur, a partir de los hallazgos identificados en su actualización, 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, delinea las rutas para una capacitación focalizada en materia protección de datos en aras de 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 Contraloría General de 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 Califoria Sur, aportando con ello certeza a la ciudadanía de cuáles son y cuál es el destino de los datos recabado por éste Órgano Estatal de Control.

## 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 la Contraloría General de 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 Contraloría General de 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 Contraloría General de 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 riegos de los datos personales que son objeto de tratamiento por la Contraloría General de 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, bloqueo y/o 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 autorizado.
- Pérdida o destrucción no autorizada.
- Otras

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 Contraloría General de 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 < = 1 | Bajo |
| Cuando > 1 y < 2 | Medio |
| Cuando el valor es > = 2 | Alto |

## 5.2 Estado actual del riesgo de datos personales

En general se tiene que la Contraloría General de Estado de Baja California Sur, cuenta con 6 unidades administrativas de nivel Dirección, en las que se da tratamiento de datos personales mediante 13 procesos prioritarios.

El promedio de riesgo que se presenta en el conjunto de procesos de los que es responsable cada una de las 6 unidades administrativas que trata datos personales en la CG, ubica en la posición más alta a la Dirección Administrativa con 1.3 seguida en forma descendente por la Dirección de Control de Obras con 1.23, Dirección de Seguimiento a Programas Federales con 1.2, la Dirección de Anticorrupción con 1.06, la Dirección Jurídica con 1, así como la Dirección de Auditoría Gubernamental.

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: 22.22%, mientras que el bloqueo recibe el mínimo porcentaje: 17.49%.

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 28.32% de los casos; seguida de Pérdida o destrucción no autorizada, con 24.78%; Uso, acceso o tratamiento no autorizado, con 23.89%, y por último Daño, alteración o modificación no autorizado, con 23.01%.

En el almacenamiento de datos personales, la amenaza más frecuente es el Daño, alteración o modificación no autorizado, con 29.14%, el Robo, extravío o copia no autorizada, con 24.78%; después la Pérdida o destrucción no autorizada, con 23.04%; y el Uso, acceso o tratamiento no autorizado, con 23.04%.

En la etapa de tratamiento de datos personales, la amenaza identificada con mayor peso es la Pérdida o destrucción no autorizada, con 23%; enseguida se encuentran con el mismo porcentaje el Robo, extravío o copia no autorizada, con 23% así como el Daño, alteración o modificación no autorizado, con 23% y por último el Uso, acceso o tratamiento no autorizado, que alcanza un 23%.

En la transferencia de datos personales, la amenaza más alta es el Uso, acceso o tratamiento no autorizado, con 31%; seguida del Daño, alteración o modificación no autorizado, con 24%, 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; Uso, acceso o tratamiento no autorizado; Daño, alteración o modificación no autorizado, y Pérdida o destrucción no autorizada, con un 25% cada una.

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 eso datos, se tiene que, de manera general, en la Contraloría General del Estado de Baja California Sur el nivel de riesgo bajo es el que predomina, debido a que es el establecido para 75% de sus procesos.

## 6. Medidas de seguridad generales.

Las medidas generales de seguridad administrativas, físicas y técnicas con las que actualmente cuenta la CG 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 a la 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, el Departamento de Informática de la Contraloría General implementa los siguientes controles:

1. Definición de políticas de contraseñas.

2. Asignación de privilegios de acuerdo a roles y funciones.

3. Tareas de respaldo por servidor.

4. Autenticación de correo electrónico.

5. Tareas de respaldo de las instancias de base de datos del servicio.

7. Acceso a los sistemas conforme a procedimiento de administración de usuarios y contraseñas con cuenta local con permiso de administrador.

8. Borrado seguro de la información que reside en los equipos de cómputo

9. Deshabilitación de cuentas de personal que causa baja.

10. Acceso controlado de administración y accesos privilegiados.

11. Definición de procedimientos y controles de seguridad de la información.

### 6.1 Monitoreo de las medidas de seguridad.

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:

1. 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.

2. 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.

3. Revisar el cumplimiento de protocolos.

4. Validar que los accesos, baja o cambio a sistemas se realicen conforme al proceso de administración de usuarios.

5. 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 Contraloría General, resultó necesario asociar dichas actividades con las facultades que el Reglamento Interior otorga a los servidores públicos 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 los servidores públicos que llevan a cabo tratamiento de datos personales dentro de las unidades administrativas que conforman la estructura orgánica de este Órgano Estatal de Control:

| Unidad responsable | Nombre y cargo del personal responsable del tratamiento de los datos | Funciones relacionadas con el tratamiento de datos | Obligaciones |
|---|---|---|---|
| Dirección Jurídica | Alfredo Machado García Director Jurídico | Artículo 15 del Reglamento Interior de la Contraloría General.<br><br>XII. Iniciar, substanciar y resolver el procedimiento de intervenciones de oficio, por presumir la inobservancia de las disposiciones en materia de adquisiciones, arrendamientos y servicios, y obras públicas y servicios relacionados con las mismas, de conformidad con las disposiciones legales aplicables;<br><br>XXI. Ejercer las atribuciones de Autoridad Substanciadora y Autoridad Resolutora que le conceda la Ley de Responsabilidades Administrativas del Estado y Municipios de Baja California Sur, en lo correspondiente a las faltas administrativas no graves;<br><br>XXIV. Ejercer las atribuciones de Autoridad Substanciadora que le conceda la Ley de Responsabilidades Administrativas del Estado y Municipios de Baja California Sur, en lo correspondiente a las faltas administrativas graves o de particulares, en el ámbito de su competencia, dirigiendo y conduciendo el procedimiento de | Recepción, registro y resguardo de los datos personales tratados. |

| | | | |
|---|---|---|---|
| | | responsabilidad administrativa desde la admisión del informe de presunta responsabilidad administrativa hasta la conclusión de la audiencia inicial, enviando los autos originales del expediente al Tribunal de Justicia Administrativa del Estado de Baja California Sur; | |
| Dirección Jurídica | Alfredo Machado García Director Jurídico | Artículo 15 del Reglamento Interior de la Contraloría General.<br><br>V. Recibir y registrar las declaraciones de situación patrimonial, de intereses y constancias de presentación de declaración fiscal de los servidores públicos de las dependencias y entidades de la Administración Pública Estatal, así como verificar su contenido mediante las investigaciones que resulten pertinentes de acuerdo con las disposiciones aplicables; | Recepción, registro y resguardo de los datos personales tratados. |
| Dirección de Anticorrupción | Ana Carolina Rosas García Directora de Anticorrupción | Artículo 21 del Reglamento Interior de la Contraloría General.<br><br>XVI. Integrar el Expediente de Presunta Responsabilidad Administrativa derivado de la investigación de denuncias y resultados de auditorías, posiblemente constitutivos de faltas administrativas; | Recepción, registro y resguardo de los datos personales tratados. |
| Dirección de Anticorrupción | Ana Carolina Rosas García Directora de Anticorrupción | Artículo 21 del Reglamento Interior de la Contraloría General.<br><br>XXIX. Elaborar y promover programas de capacitación y sensibilización en materia de ética, integridad y prevención de conflictos de interés, a los integrantes de | Recepción, registro y resguardo de los datos personales tratados. |

| | | | |
|---|---|---|---|
| | | los Comités de Ética en las Dependencias y Entidades de la Administración Pública Estatal, así como para los servidores públicos, municipios y demás instituciones públicas y/o sectores privado y social, previo convenio de colaboración que al efecto se celebre con dichas autoridades locales e instituciones | |
| Dirección de Seguimiento a Programas Federales | Servando Espinoza Villavicencio Director de Seguimiento a Programas Federales | Artículo 19 del Reglamento Interior de la Contraloría General.<br><br>II. Fungir como enlace con la Secretaría de la Función Pública, Auditoría Superior de la Federación, Auditoría Superior del Estado de Baja California Sur y unidades administrativas de esta Contraloría, en el inicio y práctica de las auditorías que se efectúen por parte de dichas entidades de fiscalización superior, así como de las observaciones y requerimientos que le realicen a esta Entidad Federativa; | Recepción, registro y resguardo de los datos personales tratados. |
| Dirección de Seguimiento a Programas Federales | Servando Espinoza Villavicencio Director de Seguimiento a Programas Federales | Artículo 19 del Reglamento Interior de la Contraloría General.<br><br>VIII. Dar seguimiento hasta su solventación, a las observaciones y recomendaciones generadas, por la Secretaría de la Función Pública, Auditoría Superior de la Federación y la Auditoría Superior del Estado de Baja California Sur, a las Dependencias y Órganos Descentralizados, de la | Recepción, registro y resguardo de los datos personales tratados. |

| | | | |
|---|---|---|---|
| | | Administración Pública Estatal; | |
| Dirección de Control de Obras | David Torres Mendoza Director de Control de Obras | Artículo 11 del Reglamento Interior de la Contraloría General.<br><br>XIII. Auditar y fiscalizar el uso de fondos en programas de inversión pública del Gobierno Estatal y los que la Federación transfiera al Estado para su ejercicio y los que éste a su vez transfiera a los Municipios, así como los que se deriven de convenios y/o programas signados con la Federación; | Recepción, registro y resguardo de los datos personales tratados. |
| Dirección de Control de Obras | David Torres Mendoza Director de Control de Obras | Artículo 11 del Reglamento Interior de la Contraloría General.<br><br>III. Revisar las convocatorias, bases de licitación y modelo de contrato para su publicación a través del sistema electrónico de contrataciones gubernamentales denominado Compranet; | Recepción, registro y resguardo de los datos personales tratados. |
| Dirección Administrativa | Mónica Aguirre Rosales Directora Administrativa | Artículo 11 del Reglamento Interior de la Contraloría General. | Recepción, registro y resguardo de los datos personales tratados. |
| Dirección Administrativa | Mónica Aguirre Rosales Directora Administrativa | Artículo 11 del Reglamento Interior de la Contraloría General.<br><br>VI. Establecer, de conformidad con los Lineamientos aplicables, las políticas y procedimientos para la administración de los recursos humanos, materiales y financieros de la Contraloría General, y difundirlas entre las | Recepción, registro y resguardo de los datos personales tratados. |

| | | | |
|---|---|---|---|
| | | unidades administrativas de la misma; | |
| Dirección de Auditoría Gubernamental | Itzel Alexandra Ortega Ojeda Directora de Auditoría Gubernamental | Artículo 13 del Reglamento Interior de la Contraloría General.<br><br>I. Efectuar auditorías, supervisiones, verificaciones, revisiones y visitas a las dependencias y entidades de la Administración Pública del Estado, tendientes a:<br><br>a) Verificar que se ajusten sus actos a las disposiciones legales aplicables en el despacho de los asuntos de sus respectivas competencias;<br><br>b) Comprobar la razonabilidad de la información financiera;<br><br>c) Proponer las acciones que fueren necesarias para el mejoramiento de la eficiencia y logro de sus objetivos en las operaciones;<br>d) Verificar que las operaciones sean congruentes con los procesos aprobados de planeación, programación y presupuestación; y<br><br>e) Comprobar el cumplimiento de las disposiciones en materia de registro, contabilidad, contratación de servicios, pagos de personal, adquisiciones, arrendamientos, | Recepción, registro y resguardo de los datos personales tratados. |

| | | | |
|---|---|---|---|
| | | conservación, uso, destino, afectación, enajenación, baja de bienes muebles e inmuebles, donaciones almacenaje y demás activos y recursos materiales y financieros del Gobierno del Estado. | |
| Dirección de Auditoría Gubernamental | Itzel Alexandra Ortega Ojeda Directora de Auditoría Gubernamental | Artículo 13 del Reglamento Interior de la Contraloría General.<br><br>XXIX. Coordinar los trabajos de los Órganos Internos de Control o sus equivalentes, y demás unidades de apoyo técnico-operativo que las integran, en las dependencias y entidades de la Administración Pública Estatal, y requerir la información necesaria para supervisar las actividades de las mismas; | Recepción, registro y resguardo de los datos personales tratados. |
| Dirección de Auditoría Gubernamental | Itzel Alexandra Ortega Ojeda Directora de Auditoría Gubernamental | Artículo 13 del Reglamento Interior de la Contraloría General.<br><br>III. Vigilar el cumplimiento, por parte de las dependencias y entidades de la Administración Pública del Estado, de las obligaciones fiscales, patronales, en materia de planeación, presupuestación, ingresos, financiamiento, inversión, deuda, patrimonio, fondos y valores, propiedad o al cuidado del Gobierno del Estado; | Recepción, registro y resguardo de los datos personales tratados. |

## 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.

- Promover un sistema de gestión y administración de datos personales que permita centralizar mediante la identificación de datos por categorías, asociando los diversos tratamientos y procesos a las políticas de seguridad que resultan aplicables a cada caso, conforme a los estándares y mejores prácticas en la materia.

- 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.