



**SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS  
DATOS PERSONALES DEL INSTITUTO DE  
TRANSPARENCIA, ACCESO A LA INFORMACIÓN  
PÚBLICA Y PROTECCIÓN DE DATOS DEL ESTADO  
DE COLIMA**

## CONTENIDO

<b>1.- PRESENTACIÓN.....</b>	<b>1</b>
<b>2.-SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS DATOS PERSONALES.....</b>	<b>4</b>
2.1 Definiciones.....	4
2.2 ¿Qué es un Sistema de Gestión?.....	8
<b>3. ACCIONES PARA LA SEGURIDAD DE LOS DATOS PERSONALES.....</b>	<b>9</b>
<b>Primera Fase.</b>	
3.1 Planeación del SGSDP.....	9
3.2 Alcance y Objetivos.....	11
3.3 Política de Gestión de Datos Personales.....	12
3.4 Funciones y Obligaciones de Quienes Traten Datos Personales.....	16
3.5 Inventarios de Datos Personales del INFOCOL.....	19
3.6 Análisis de Riesgo de los Datos Personales.....	23
3.7 Medidas de seguridad y Análisis de Brecha.....	29
<b>Segunda Fase.</b>	
3.8 Implementación y operación del SGSDP.....	44
3.9 Implementación de las Medidas de Seguridad Aplicables a los Datos Personales.....	45
3.10 Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.....	48
<b>Tercera Fase.</b>	
3.11 Monitoreo y Revisión del SGSDP.....	58
3.12 Revisiones y Auditorías.....	58
<b>Cuarta Fase.</b>	
3.13 Mejorar el SGSDP.....	62
3.14 Mejora Continua y Capacitación.....	63

## 1. PRESENTACIÓN

Al igual que las otras herramientas normativas como el Documento de Seguridad, que mandata desarrollar la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y nuestra ley local en la materia para cada entidad pública de nuestro Estado que sea sujeto obligado, se reconoce de manera indubitable, que la información es un activo que, al igual que sus instalaciones, capital humano y recursos financieros, debe protegerse mediante un conjunto coherente de procesos y sistemas diseñados, bien administrados por la propia entidad pública que busque establecer, implementar, operar, monitorear y mejorar los procesos y sistemas relativos a la confidencialidad, integridad y disponibilidad de la información, aplicando un enfoque basado en los riesgos que se afrontan; llevando a cabo una correcta administración de riesgos a fin de que éstos puedan ser asumidos y mitigados de manera eficiente, sistemática y estructurada, que se adapte a los cambios que se produzcan en el entorno y en la información.

Como es bien sabido, actualmente se posibilita la recolección y almacenamiento de grandes volúmenes de información en pequeños dispositivos y facilita su transmisión por medios remotos a grandes distancias en cuestión de segundos, por lo tanto se facilitan también los riesgos de vulneraciones diversas al interior de la institución. En este sentido, al incluirse el tratamiento de información relativa o concerniente a personas físicas, en cada entidad pública de nuestro Estado que es sujeto obligado por la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima; se actualiza la competencia y atribución del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima (INFOCOL), en su calidad de órgano garante, para velar por la protección de estos datos personales en el ámbito de la administración pública estatal.

Como sabemos, las vulneraciones de seguridad generan altos costos institucionales además de afectaciones en la esfera de otros derechos y libertades fundamentales de las personas. Es por ello que no resulta conveniente escatimar recursos y esfuerzos en el establecimiento de controles para la protección de la información frente a acciones o situaciones no deseadas, pues de esa manera, además de garantizar la continuidad de la operación de los sujetos obligados, se protege a los individuos a los que se refiere dicha información. Por lo anterior, para efecto de conocer el tipo de controles a que se hace referencia, éstos deben estar documentados, estructurados y ser difundidos para el conocimiento de todos los involucrados en el tratamiento de la información en cada entidad pública responsable en nuestro Estado, de conformidad con la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima.

A este respecto, nuestra ley en la materia antes referida, en su Capítulo II DE LOS DEBRES, define en su artículo 43 al Sistema de Gestión para las Medidas de Seguridad de los Datos Personales, el cual guarda una estrecha relación con las acciones relacionadas a la gestión de las medidas de seguridad para el tratamiento de los datos personales, pues estas a su vez, deberán estar documentadas y contenidas en un sistema de gestión propiamente. Es en este sentido, que se entenderá 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, de conformidad con lo previsto en esta ley y las demás disposiciones que resulten aplicables en la materia.

Por lo anterior, el Sistema de Gestión de Seguridad de los Datos Personales, o para las medidas de seguridad como lo marca nuestra la ley, es pues, un instrumento normativo en el cual de manera exhaustiva, y derivado de un profundo análisis al interior de nuestra institución pública, se describen los procesos que

conlleva “Planificar-Hacer-Verificar-Actuar” según la metodología (PHVA), para gestionar con éxito lo relacionado a la implementación y seguimiento de las medidas de seguridad administrativas, físicas y técnicas, para garantizar la adecuada protección del tratamiento de datos personales que se recaban, gestionan y resguardan al interior de la misma.

## 2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS DATOS PERSONALES

### 2.1 Definiciones

**Activo.** La información, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para nuestra institución u organización.

**Bases de datos.** El conjunto ordenado de datos personales referentes a una persona física identificada o identificable.

**Datos personales:** Cualquier información 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;

**Datos personales sensibles:** Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

**Encargado:** La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trate datos personales a nombre y por cuenta del responsable;

**Impacto.** Una medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

**Incidente.** Escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades.

**Amenaza.** Circunstancia o evento con la capacidad de causar daño a una organización.

**Vulnerabilidad.** Falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas.

**Responsable:** Los sujetos obligados a que se refiere el artículo 3, párrafos segundo y tercero de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima, que deciden sobre el tratamiento de datos personales, así como al definición de los fines, medios, alcances y demás cuestiones relacionadas con el tratamiento de datos personales;

**Riesgo.** Combinación de la probabilidad de un evento y su consecuencia desfavorable.

**Riesgo de seguridad.** Potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización.

**Identificar el riesgo.** Proceso para encontrar, enlistar y describir los elementos del riesgo.

**Valorar el riesgo.** Proceso para asignar valores a la probabilidad y consecuencias del riesgo.

**Comunicar el riesgo.** Compartir o intercambiar información entre la alta dirección, custodios y demás involucrados acerca del riesgo.

**Tratar el riesgo:** Procesos que se realizan para modificar el nivel de riesgo.

**Aceptar el riesgo.** Decisión informada para coexistir con un nivel de riesgo.

**Compartir el riesgo.** Proceso donde se involucra a terceros para mitigar la pérdida generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad.

**Evitar el riesgo.** Acción para retirarse de una situación de riesgo o decisión para no involucrarse en ella.

**Reducir el riesgo.** Acciones tomadas para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas al riesgo.

**Retención del riesgo.** Aceptación de la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido.

**Riesgo residual.** El riesgo remanente después de tratar el riesgo.

**Seguridad de la información.** Preservación de la confidencialidad, integridad y disponibilidad de la información, así como otras propiedades delimitadas por la normatividad aplicable.

**Confidencialidad.** Los controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.

**Integridad.** La propiedad de salvaguardar la exactitud y completitud de los activos.

**Sistema de Gestión de Seguridad de Datos Personales (SGSDP).**

Se entenderá 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, de conformidad con lo previsto en esta ley y las demás disposiciones que resulten aplicables en la materia.

**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, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales;

**Transferencia:** Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;



## 2.2 ¿Qué es un sistema de Gestión?

La gestión es un conjunto de actividades coordinadas para dirigir y controlar un proceso o tarea. Un sistema es un conjunto de elementos mutuamente relacionados o que interactúan por un fin u objetivo. Por lo tanto, un Sistema de Gestión (SG) se define como un conjunto de elementos y actividades interrelacionadas para establecer metas y los medios de acción para alcanzarlas.

Asimismo, un sistema de gestión apoya en este caso a las instituciones públicas, en la dirección, operación y control de forma sistemática y transparente de sus procesos, a fin de lograr con éxito sus actividades, ya que está diseñado para mejorar continuamente el desempeño de un organización, mediante la consideración de las necesidades de todas las partes interesadas.

Es importante tomar en cuenta que la institución tiene que definir y gestionar numerosas actividades para funcionar con eficiencia. Estas actividades se convierten en procesos que tienen la característica de recibir elementos de entrada, los cuales se gestionan para regresar al final de su ciclo, como elementos de salida (resultados). Por ejemplo, un proceso de Auditoría puede recibir como elementos de entrada objetivo, alcance y plan de auditoría, así como el informe de resultados de la auditoría anterior, y como elemento de salida un nuevo informe de auditoría. A menudo, la salida de un proceso se convierte directamente en la entrada del proceso siguiente, y la interconexión entre procesos genera sistemas que se retroalimentan para mejorar.

En el caso de las Recomendaciones en materia de Seguridad de los Datos Personales, emitidas por el INAI, el sistema de gestión propuesto se basa en el modelo denominado “Planificar-Hacer-Verificar-Actuar” (PHVA), a través del cual se dirigen y controlan los procesos o tareas, como se puede ver en la tabla 1 y figura 1:

	Elemento del SG	Fase del PHVA	Actividades
PROCESO	Metas	Planificar	Se identifican políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por la organización (meta).
	Medios de acción	Hacer	Se implementan y operan las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
		Verificar	Se evalúan y miden los resultados de las políticas, objetivos, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.
		Actuar	Se adoptan medidas correctivas y preventivas, en función de los resultados y de la revisión, o de otras informaciones relevantes, para lograr la mejora continua.

Tabla 1. Sistema de Gestión

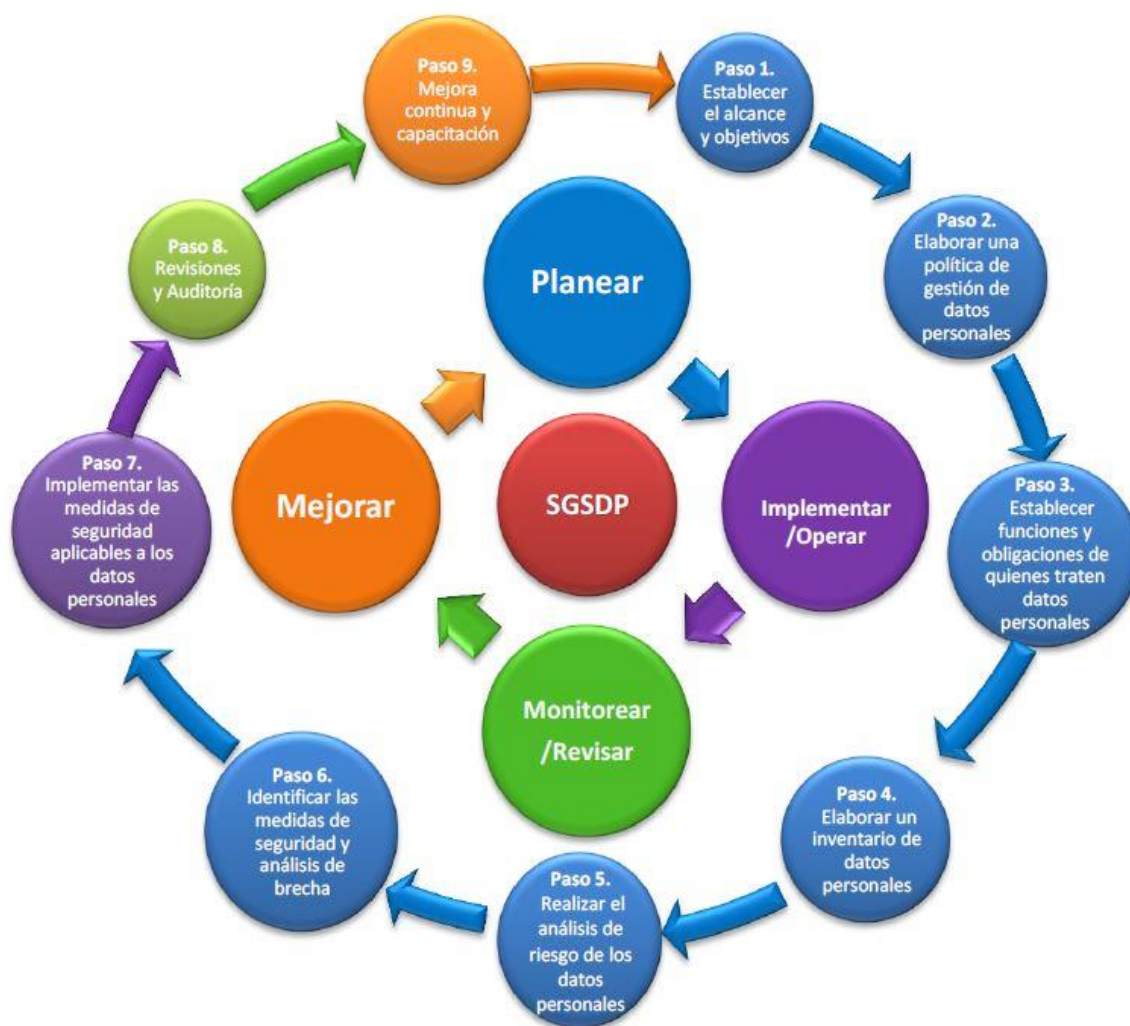
### 3. ACCIONES PARA LA SEGURIDAD DE LOS DATOS PERSONALES.

#### Primera Fase

##### 3.1 Planeación del SGSDP

El presente documento de desarrolla en cuatro fases, por su puesto la primera es la fase de **Planeación** del SGSDP, donde se establecen los objetivos y procesos necesarios para llegar a la meta u obtener los resultados esperados por la

institución, en este caso en particular, la protección y seguridad de los datos personales. El siguiente esquema resume y clarifica todo el proceso ordenado y circular que va de la planeación a la consecución del sistema, para comenzar de nuevo bajo el esquema propuesto por la metodología PHVA, que implica Planificar-Hacer-Verificar-Actuar, como se muestra a continuación:



## 3.2 Objetivos

### **General.**

Tener establecido en el presente documento, denominado Sistema de Gestión de Seguridad de los Datos Personales, la dirección, operación y control de forma sistemática y transparente de los procesos que involucren la gestión y resguardo de datos personales en las diferentes áreas del INFOCOL; a fin de contar con los protocolos y actividades de seguridad necesarias para su protección.

### **Objetivos específicos.**

- 1.- Tener clara la política de gestión de los datos personales al interior del INFOCOL.
2. Determinar y describir las funciones y obligaciones de quienes traten los datos personales en la institución.
3. Estructurar los inventarios de datos personales por cada área del INFOCOL que los recabe y gestione.
4. Realizar el análisis de riesgos de la institución, a los que están sujetos los datos personales, basados en la metodología BAA ( Beneficio – Accesibilidad – Anonimidad).
- 5.- Identificar y describir las medidas de seguridad Técnicas, Físicas, Administrativas, derivado del análisis de riesgos y análisis de brecha realizado al interior del INFOCOL.
- 6.- Aplicación del procedimiento de mejora continua y actualización, bajo la estrategia PHVA (Planificar-Hacer-Verificar-Actuar).

### **3.3 Política de Gestión de Datos Personales**

Toda vez que se han descrito y aprobado por el Pleno del INFOCOL las Políticas de Gestión de los Datos Personales contenidas en el presente documento, se vuelven parte esencial de nuestro Sistema de Gestión, al ser de observancia obligatoria para todos los servidores públicos al interior de la institución, que en el ejercicio de sus funciones realicen 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, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, de conformidad con el artículo 4 fracción XXXII de la ley antes referida, y en estricta concordancia con el cumplimiento a los propios principios y deberes que de ella emanan.

#### ***Cumplimiento de los Principios y Deberes en materia de Protección de Datos Personales.***

##### ***Principios.***

Haciendo un ejercicio arbitrario de interpretación, la parte moral y ética de la propia Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima, es precisamente dar cumplimiento a todos los principios que establece el artículo 15 de la Ley:

- I. Licitud;
- II. Finalidad;
- III. Lealtad;
- IV. Consentimiento;
- V. Calidad;
- VI. Proporcionalidad;
- VII. Información; y
- VIII. Responsabilidad en el tratamiento de los datos personales.

- I) Tratar y recabar datos personales de manera lícita, conforme a las disposiciones establecidas por la Ley y demás normativa aplicable (principio de licitud);
- II) Limitar el tratamiento de los datos personales al cumplimiento de las finalidades previstas en el aviso de privacidad (principio de finalidad);
- III) No obtener los datos personales a través de medios fraudulentos (principio de lealtad);
- IV) Sujetar el tratamiento de datos personales al consentimiento del titular, salvo las excepciones previstas por la Ley (principio de consentimiento);
- V) Procurar que los datos personales tratados sean correctos y actualizados; suprimir los datos personales cuando hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y para las cuales se obtuvieron; tratar datos personales estrictamente el tiempo necesario para propósitos legales, regulatorios o legítimos organizacionales (principio de calidad);
- VI) Tratar los menos datos personales posibles, y sólo aquéllos que resulten necesarios, adecuados y relevantes en relación con las finalidades previstas en el aviso de privacidad (principio de proporcionalidad);
- VII) Informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad (principio de información);
- VIII) Velar por el cumplimiento de estos principios y adoptar las medidas necesarias para su aplicación (principio de responsabilidad);

### ***Deberes.***

Por otra parte, se encuentran los Deberes en materia de Protección de Datos Personales, estipulados en los artículos del 38 al 49 de nuestra ley en la materia. El Deber de Seguridad y de Confidencialidad en este sentido, nos obliga a tener herramientas normativas bien definidas para la prevención y actuación en caso de vulneraciones y fallas en las medidas de seguridad para la protección de los datos, entre otras cosas:

- a) Establecer y mantener medidas de seguridad (deber de seguridad);
- b) Guardar la confidencialidad de los datos personales (deber de confidencialidad);
- c) Identificar el flujo y ciclo de vida de los datos personales: por qué medio se recaban, en qué procesos de nuestra institución se utilizan, con quién se comparten, y en qué momento y por qué medios se suprimen;
- d) Mantener un inventario actualizado de los datos personales o de sus categorías que maneja la institución;
- e) Respetar los derechos de los titulares en relación con sus datos personales;
- f) Aplicar las excepciones contempladas en la normativa en materia de protección de datos personales;
- g) Desarrollar e implementar un Sistema de gestión de Seguridad de los Datos Personales (SGSDP) de acuerdo a la política de gestión de datos personales, y
- h) Definir las partes interesadas y miembros de la institución con responsabilidades específicas y a cargo de la rendición de cuentas para el (SGSDP).

### **Controles para garantizar que se valida la confidencialidad, integridad y disponibilidad de los datos personales.**

La Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados para el Estado de Colima, establece en su artículo 40, que los responsables deben garantizar la confidencialidad, integridad y disponibilidad de los datos personales en su posesión; lo anterior, a través de las medidas de seguridad, más específicamente de las medidas de seguridad Técnicas, Físicas y Administrativas.

### **Controles de Confidencialidad.**

- Como medida de control primordial, todo el personal del INFOCOL deberá guardar confidencialidad permanente de los datos personales a los que tenga acceso.

- Para formalizar el mecanismo anterior, todo el personal deberá firmar carta compromiso de confidencialidad en este sentido.
- Se podrán desclasificar datos personales solo en los casos que la Leyes en la materia señalen.
- La Secretaría de Protección de Datos Personales del INFOCOL impartirá capacitaciones periódicas para todo su personal, en materia de medidas de seguridad para la protección de datos personales.
- El personal está obligado a cumplir con las medidas de seguridad físicas, técnicas y administrativas señaladas en el Documento de Seguridad.
- Se realizará una revisión periódica de las medidas de seguridad; físicas, técnicas y administrativas del instituto.

#### ***Controles de Integridad.***

- Los datos personales deberán conservarse en el estado en que son recabados, asimismo los documentos que resulten del aprovechamiento de los datos personales deberán ser conservar su integridad.
- El personal conservará los datos personales que se encuentren en formato físico conforme a lo señalado por las medidas de seguridad físicas contenidas en el Documento de Seguridad.
- El personal conservará los datos personales que se encuentren en formato electrónico conforme a lo señalado por las medidas de seguridad técnicas contenidas en el Documento de Seguridad.
- El personal deberá mantener un formato de inventario de datos personales permanente y actualizado, de tal manera que se describa e identifique plenamente los tipos de dato que gestiona y debe proteger.

#### ***Controles de Disponibilidad.***

- Se realizará una digitalización completa de la información que ingresa a través de la oficialía de partes y se almacena en discos duros.



- Una operación de respaldo incremental solo copia los datos que han variado desde la última operación de respaldo de cualquier tipo. Se utiliza la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último respaldo.
- Deberá realizarse un respaldo incremental de la información de cada área 1 vez al mes y almacenarlo en discos duros.
- Cada área será la responsable de almacenar sus respaldos durante el tiempo que señale el catálogo de disposición documental del Instituto, atendiendo, a las recomendaciones de la Secretaría de Archivos, así como de la Secretaría de Protección de Datos Personales del INFOCOL.

### **3.4 Funciones y Obligaciones de Quienes Traten Datos Personales**

Para efecto de que el personal que recaba, gestiona y da tratamiento a los datos personales dentro de la institución, tenga claro sus funciones y responsabilidades hacia el propio tratamiento de los mismos, es necesario que tenga plenamente identificado el tipo de datos que maneja, y cual es el nivel de protección que se requiere.

Para lo anterior, el documento de seguridad eséfica los instrumentos y controles necesarios para este fin, a través de las bitácoras de operación cotidiana, formato de registro de vulneraciones y los inventarios de datos personales por área que gestiona los mismos, lo cual permite tener plenamente identificado el responsable de las bases de datos, los tipos de datos que se gestionan, así como los alcances y limitaciones para su tratamiento. En este sentido se hace énfasis en la descripción y características de los siguientes instrumentos:

***Bitácoras de Acceso, Operación Cotidiana y Vulneraciones a la Seguridad de los Datos Personales.***

## **1.- Bitácoras de Acceso.**

1. Las bitácoras de acceso a los datos personales se utilizan en los soportes físicos y contienen la siguiente información:

- Nombre y cargo de quien accede
- Identificación del Expediente
- Fojas del Expediente
- Propósito del Acceso
- Fecha de Acceso
- Hora de Acceso
- Fecha de Devolución
- Hora de Devolución

2. Las áreas de este instituto, que administran bitácoras de acceso a los datos personales en soportes físicos son las siguientes:

- Secretaría de Administración.
- Secretaría de Acuerdos.
- Unidad de Transparencia.
- Órgano Interno de Control

3. Resguardadas por los titulares de cada área:

- Lic. Nora Hilda Chávez Ponce. Secretaria de Administración.
- Lic. César Margarito Alcántar García. Secretario de Acuerdos.
- Mtro. Mauricio Zuazo Rueda. Titular del Órgano Interno de Control.
- Mtro. Juan Carlos González Torres. Encargado de la Unidad de Transparencia.

## **2.- Bitácoras de vulneraciones a la seguridad de los datos personales.**

1. La bitácora de vulneraciones contiene la siguiente información:

- Nombre de quien reporta el incidente.
- Cargo.
- La fecha en la que ocurrió.
- El motivo de la vulneración de seguridad; y

- Las acciones correctivas implementadas de forma inmediata y definitiva.
2. Las áreas que por su gestión con datos personales contendrán bitácoras de vulneraciones son las siguientes:
- Secretaría de Administración.
  - Secretaría de Acuerdos.
  - Unidad de Transparencia.
  - Órgano Interno de Control

***Controles de Identificación y Autenticación de Usuarios.***

Para cumplir con este objetivo, a continuación se señala y se detalla la forma en que se identifica al personal del INFOCOL, así como la forma en que se autentifica a cada uno.

1.- Los empleados de la Secretaría deben portar en todo momento su identificación institucional que cuenta con la siguiente información:

Al frente:

- Nombre
- Cargo

Al reverso:

- Vigencia
- Número de Empleado
- Firma del Titular de la Institución
- Sitio Oficial
- RFC
- Domicilio de la Institución
- Teléfono de la Institución

2.- En el ámbito electrónico, todas las computadoras precisan de un nombre de usuario y contraseña para ingresar por parte del encargado. También de manera electrónica se lleva a cabo el registro y actualización en su caso de los inventarios de datos personales por cada área del instituto que recaba y gestiona los mismos.

## 3.5 Inventarios de Datos Personales del INFOCOL

### INVENTARIO DP SECRETARIA DE ADMINISTRACIÓN

Tipo de Datos Personales	Medio de obtención de los datos personales	Listado de Datos Personales	Sensible	Formato de la base de datos	Sistema de Tratamiento	Ubicación base de datos	Finalidades del tratamiento	¿Requiere consentimiento?	Tipo de consentimiento	Nombre del encargado, en su caso	Cargo del encargado en su caso	¿Se realizan transferencias?	Si la respuesta es SI, indicar la finalidad	Indicar si las transferencias requieren consentimiento
Indicar el tipo de Datos Personales a los cuales se les otorga un tratamiento en institución.	Señalar el o los medios a través de los cuales se obtienen los datos personales en esta institución. Si se trata de un medio, se deberá indicar un medio por fila.	Indicar cada uno de los datos personales que se tratan o sus categorías, uno por fila.	Señalar si el dato personal es sensible.	Señalar el formato en el cual se encuentra la base de datos.	Señalar el sistema mediante el cual se procesan los datos personales (Físico o electrónico).	Señalar la ubicación de la base de datos y si es más de una, indicar una por fila.	Indicar cada uno de los fines del tratamiento, los cuales deberán ser expuestos por separado. Una por fila.	Indicar si la finalidad requiere o no el consentimiento del titular.	En caso de que la finalidad requiera el consentimiento del titular, señalar el tipo de consentimiento que se necesita.	Señalar nombre de la persona física o moral que actúa como encargada en el tratamiento, en su caso. Una por fila.	Señalar el cargo de la persona física o moral que actúa como encargada en el tratamiento.	Señalar si se realizan transferencias de los datos personales en el marco del tratamiento.	Indicar con qué finalidad se realizan las transferencias de los datos personales que se tratan.	Indicar con base en la Ley 1712 de 2014, si las transferencias requieren consentimiento.
Datos identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Nombre de la persona	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Acta de nacimiento	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	CURP	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Datos de la Credencial de Director (Domicilio, unidad federativa, clave de elector, número OCR).	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Teléfono particular	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Firma	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Fotografía	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos sobre Salud	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Número de Seguridad Social	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	RFC	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Académicos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Curriculum Vitae	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Académicos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Título o documento que acredite el grado académico	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Académicos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Cédula profesional	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Laborales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Nombre de la empresa	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Laborales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Área de desempeño	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Laborales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Puesto	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Laborales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Función Principal	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Laborales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Fecha de inicio	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Laborales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Fecha de término	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Laborales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Años de experiencia	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos Laborales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Años de experiencia	No	Físico	Físico	Archivos de la unidad administrativa	Recabar el expediente único del personal que labora en el INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos de Tarjeta Bancaria	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Número de Cuenta	No	Electrónico	Físico y electrónico	Equipo de cómputo	Transferir el pago quincenal a los empleados del INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA
Datos de Tarjeta Bancaria	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso.	Clave bancaria	No	Electrónico	Físico y electrónico	Equipo de cómputo	Transferir el pago quincenal a los empleados del INFOCOL.	No	NA	Nora Hilda Chávez Ponce	Secretaría Administrativa del INFOCOL	No	NA	NA

## INVENTARIO DP ORGANO INTERNO DE CONTROL DEL INFOCOL

Tipo de Dato Personal	Medio de obtención de los datos personales	Listado de Datos Personales	Sensible	Formato de la base de datos	Sistema de Tratamiento	Ubicación base de datos	Finalidades del tratamiento	¿Requiere consentimiento?	Tipo de consentimiento	Nombre del encargado, en su caso	Cargo del encargado en su caso	¿Se realizan transferencias?	Si la respuesta es Si, indicar la finalidad	Indicar si las transferencias requieren consentimiento
Indicar el tipo de Datos Personales que están en los datos personales en un momento en específico.	Indicar en la materia de los datos personales que están en los datos personales en un momento en específico.	Indicar cada uno de los datos personales que están en los datos personales en un momento en específico.	Indicar si el dato es sensible o no.	Indicar el formato en el que se almacena la base de datos de los datos personales (Fichero electrónico).	Indicar el sistema de tratamiento al que se le da acceso a los datos personales (Fichero electrónico).	Indicar la ubicación de la base de datos de los datos personales (Fichero electrónico).	Indicar cada uno de los fines de los datos personales que están en los datos personales en un momento en específico.	Indicar si la finalidad requiere el consentimiento del titular.	En caso de que la finalidad requiera el consentimiento del titular, señalar el tipo de consentimiento que se necesita.	Señalar nombre de la o las personas físicas o morales que actúan como encargados en el momento en que se realiza el tratamiento.	Señalar el cargo de la o las personas físicas o morales que actúan como encargados en el momento en que se realiza el tratamiento.	Indicar si se realizan transferencias en el momento en que se realiza el tratamiento.	Indicar con qué finalidad se realizan las transferencias de los datos personales que están en los datos personales en un momento en específico.	Indicar con base en las transferencias de los datos personales que están en los datos personales en un momento en específico.
Datos Identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Nombre	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Domicilio particular	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Número de teléfono particular, fijo o móvil	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Firma	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	CUIP	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Datos de la Credencial de Plector (Dirección, entidad, fecha de emisión, número de elector, número OCR)	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Estado Civil	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	RFC	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Bienes muebles	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Bienes inmuebles	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Regimen fiscal	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Obligaciones fiscales	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Declaración fiscal	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Firma electrónica	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Ingresos	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Egresos	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Cuentas bancarias	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Inversiones	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA
Datos Patrimoniales	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Referencias Personales	No	Físico	Físico	Archivos de la unidad administrativa	Recibir y registrar la información derivada de las declaraciones patrimoniales, de intereses y fiscal de los empleados del INFOCOL, para cumplir con lo estipulado en la normatividad de la materia.	No	NA	Mauricio Zuazo Rueda	Titular del Órgano Interno de Control	No	NA	NA

## INVENTARIO DP SECRETARIA DE ACUERDOS DEL INFOCOL

Tipo de Dato Personal	Medio de obtención de los datos personales	Listado de Datos Personales	Sensible	Formato de la base de datos	Sistema de Tratamiento	Ubicación base de datos	Finalidades del tratamiento	¿Requiere consentimiento?	Tipo de consentimiento	Nombre del encargado, en su caso	Cargo del encargado en su caso	¿Se realizan transferencias?	Si la respuesta es SI, indicar la finalidad	Indicar si las transferencias requieren consentimiento
Indicar el tipo de Datos Personales a los cuales se les da tratamiento en esta institución.	Señalar el o los medios a través de los cuales se obtienen los datos personales en este tratamiento. Si es más de un medio, se deberá indicar un medio por fila.	Indicar cada uno de los datos personales que se tratan o tratan, en categorías, uno por fila.	Señalar si el dato personal es sensible o no.	Señalar el formato en el que se encuentra la base de datos de tratamiento.	Señalar el tipo de sistema mediante el cual se da tratamiento a los datos personales (Físico o electrónico)	Señalar la ubicación de la base de datos. Si es más de una, se deberá indicar uno por fila.	Indicar cada una de las finalidades del tratamiento, las cuales deberán ser explícitas y concretas. Una por fila.	Indicar si la finalidad requiere o no el consentimiento del titular.	En caso de que la finalidad requiera el consentimiento del titular, señalar el tipo de consentimiento que se necesita.	Señalar nombre de la o las personas físicas o morales que actúan como encargados en el tratamiento, en su caso. Uno por fila.	Señalar el cargo de la o las personas físicas o morales que actúan como encargados en el tratamiento.	Señalar si se realizan o no transferencias de los datos personales que se tratan.	Indicar con qué finalidad se realizan las transferencias de los datos personales que se tratan.	Indicar con base en la DPPI/SEC si las transferencias realizadas requieren consentimiento.
Datos Identificativos	Internet o sistema informático	Nombre del Recurrente	No	Físico y electrónico	Físico y electrónico	Archivos de la unidad administrativa	Desahogar a nombre de recurrente, los diferentes procesos en el desahogo del Recurso de Revisión o la Denuncia en su caso.	No	NA	César Margarito Alcántar García	Secretario de Acuerdos del INFOCOL	No	NA	NA
Datos Identificativos	Internet o sistema informático	Correo electrónico particular del recurrente	No	Físico y electrónico	Físico y electrónico	Archivos de la unidad administrativa	Notificar al recurrente, acerca de los diferentes procesos en el desahogo del Recurso de Revisión o de la Denuncia en su caso.	No	NA	César Margarito Alcántar García	Secretario de Acuerdos del INFOCOL	No	NA	NA
Datos Identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Datos de la Credencial de Elector (Domicilio, entidad federativa, clave de elector, número OCR).	No	Físico y electrónico	Físico y electrónico	Archivos de la unidad administrativa	Cumplir con los requisitos de identificación y sustanciación del Recurso de Revisión y la Denuncia en materia de Datos Personales.	No	NA	César Margarito Alcántar García	Secretario de Acuerdos del INFOCOL	No	NA	NA

## INVENTARIO DP UNIDAD DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA DEL INFOCOL

Tipo de Dato Personal	Medio de obtención de los datos personales	Listado de Datos Personales	Sensible	Formato de la base de datos	Sistema de Tratamiento	Ubicación base de datos	Finalidades del tratamiento	¿Requiere consentimiento?	Tipo de consentimiento	Nombre del encargado, en su caso	Cargo del encargado en su caso	¿Se realizan transferencias?	Si la respuesta es SI, indicar la finalidad	Indicar si las transferencias requieren consentimiento
Indicar el tipo de Datos Personales a los cuales se les da tratamiento en institución.	Señalar el o los medios a través de los cuales se obtienen los datos personales en este tratamiento. Si es más de un medio, se deberá indicar un medio por fila.	Indicar cada uno de los datos personales que se tratan o sus categorías, uno por fila.	Señalar si el dato personal es sensible o no.	Señalar el formato en el que se encuentra la base de datos de tratamiento.	Señalar el tipo de sistema mediante el cual se da tratamiento a los datos personales (Físico o electrónico)	Señalar la ubicación de la base de datos. Si es más de una, se deberá indicar uno por fila.	Indicar cada una de las finalidades del tratamiento, las cuales deberán ser explícitas y concretas. Una por fila.	Indicar si la finalidad requiere o no el consentimiento del titular.	En caso de que la finalidad requiera el consentimiento del titular, señalar el tipo de consentimiento que se necesita.	Señalar nombre de la o las personas físicas o morales que actúan como encargados en el tratamiento, en su caso. Uno por fila.	Señalar el cargo de la o las personas físicas o morales que actúan como encargados en el tratamiento.	Señalar si se realizan o no transferencias de los datos personales que se tratan.	Indicar con qué finalidad se realizan las transferencias de los datos personales que se tratan.	Indicar con base en la LOPPPSOCC si las transferencias realizadas requieren consentimiento.
Datos Identificativos	Internet o sistema informático	Nombre del particular	No	Electrónico	Electrónico	Equipo de cómputo	Se recaba con la finalidad de asesorar y apoyar a las personas en la realización de una solicitud o trámite de Acceso a la Información Pública o Datos Personales.	No	NA	Juan Carlos González Torres	Unidad de Transparencia del INFOCOL	No	NA	NA
Datos Identificativos	Internet o sistema informático	Correo electrónico particular	No	Electrónico	Electrónico	Equipo de cómputo	Se recaba con la finalidad de asesorar y apoyar a las personas en la realización de una solicitud o trámite de Acceso a la Información Pública o Datos Personales.	No	NA	Juan Carlos González Torres	Unidad de Transparencia del INFOCOL	No	NA	NA
Datos Identificativos	Internet o sistema informático	Correo electrónico particular	No	Electrónico	Electrónico	Equipo de cómputo	Se recaba con la finalidad de tener un medio alternativo para notificar las respuestas a las solicitudes de información pública que realizan a este instituto.	No	NA	Juan Carlos González Torres	Unidad de Transparencia del INFOCOL	No	NA	NA
Datos Identificativos	De manera personal con la presencia física del titular de los datos personales o su representante, en su caso	Credencial de Elector	No	Físico	Físico	Archivos de la unidad administrativa	Se recaba con la finalidad de cumplir con el requisito de identificación del titular de los datos personales, al momento de realizar una solicitud de derechos ARCO.	No	NA	Juan Carlos González Torres	Unidad de Transparencia del INFOCOL	No	NA	NA

### 3.6 Análisis de Riesgo de los Datos Personales.

Como se ha descrito de manera exhaustiva en el Documento de Seguridad para la Protección de los Datos Personales del INFOCOL; el análisis de riesgos en el tratamiento de los datos personales, se sustenta en la **Metodología BAA** (Beneficio, Accesibilidad y Anonimidad del atacante); esta metodología en particular, contempla tres factores que en conjunto determinan el riesgo latente de los datos personales:

- **Beneficio, factor** que deriva en el nivel de **riesgo por tipo de dato**, determinado por el riesgo inherente del dato y el volumen de titulares de las que se tratan datos.
- **Accesibilidad, factor** que determina el nivel de **riesgo por tipo de acceso**, es decir, el número de accesos potenciales a los datos.
- **Anonimidad, factor** que determina el nivel de **riesgo por tipo de entorno** desde el que se tiene acceso a los datos.

La escala de ponderación y análisis, plantea el parámetro de medición de Nivel < > (menor que – mayor que) en esta metodología, la cual se esquematiza mediante la categorización de números del **1 al 5**, en donde **1** implica **bajo** y **4, 5** implica **Reforzado**, dependiendo del tipo dato, el nivel de riesgo inherente, la anonimidad del atacante y la cantidad de titulares de datos personales que está en juego, enfatizando con la siguiente coloración específica:

Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares				
		<500k	<5k	<50k	<500k	>500k
Ubicación en conjunto con patrimoniales	REFORZADO	4	4	5	5	5
Información adicional de tarjeta bancaria	REFORZADO	4	4	5	5	5
Titulares de alto riesgo	REFORZADO	4	4	5	5	5
Salud	ALTO	1	2	3	3	3
Origen, creencias e ideológicos	ALTO	1	2	3	3	3
Ubicación	MEDIO	1	1	2	3	3
Patrimoniales	MEDIO	1	1	2	3	3
Autenticación	MEDIO	1	1	2	3	3
Jurídicos	MEDIO	1	1	2	3	3
Tarjeta Bancaria	MEDIO	1	1	2	3	3
Personales de identificación	BAJO	1	1	1	1	1



En este sentido, se especifican a continuación los tres factores asociados al nivel de riesgo por el tipo de datos, recabados y gestionados en el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del INFOCOL.

### **FACTOR Beneficio: El nivel de riesgo por tipo de dato.**

#### **Clasificación de los datos personales del INFOCOL.**

**Datos con riesgo inherente bajo.** En el caso de este Instituto de Transparencia, derivado del análisis y estructuración de los inventarios de datos personales por área ejecutiva y administrativa, se determinó que existen tres tipos de datos personales que se gestionan al interior de esta institución, que son: Datos Personales de identificación, Datos de Tarjeta Bancaria y Datos patrimoniales; en este sentido, como se puede constatar, bajo la valoración esquemática de la Metodología BAA, estos tres tipos de datos personales encuadran en los supuestos de ***Datos con riesgo inherente bajo*** y ***Datos con riesgo inherente medio*** respectivamente, bajo la consideración referida supralíneas, que atiende principalmente al tipo de dato gestionado, el riesgo y el número de titulares de datos personales que se posea. Así entonces, el esquema de valoración de las dos categorías de datos expresadas quedaría de la siguiente manera:

#### **Identificación de tipos de datos y de nivel de riesgo inherente en el INFOCOL.**

<b>Tipo de Dato</b>	<b>Nivel de riesgo inherente</b>
Personales de Identificación	<b>Bajo</b>
Patrimoniales	<b>Medio</b>
Datos de Tarjeta Bancaria	<b>Medio</b>

### Identificación de riesgo por tipo de dato.

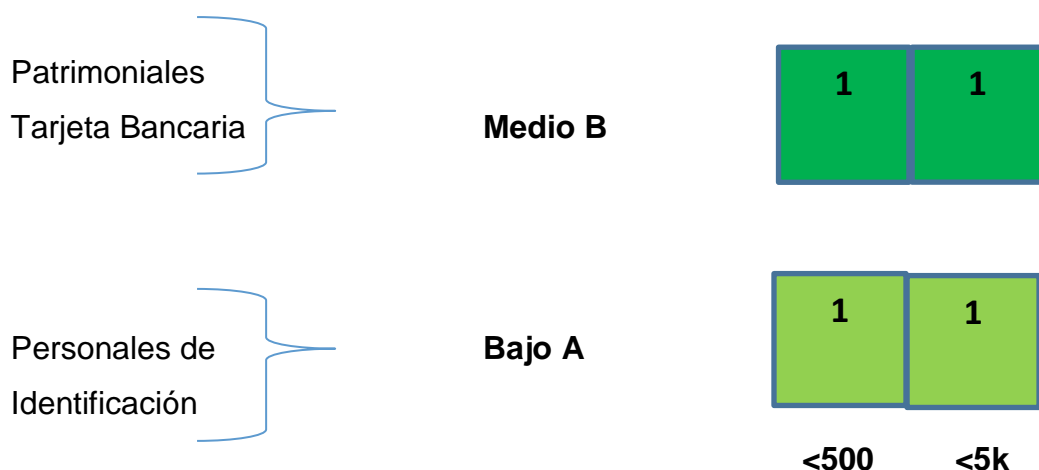
Tipo de Dato	Nivel de Riesgo Inherente	Volumen de Titulares
Personales de Identificación	Bajo	<500
Patrimoniales	Medio	<500
Datos de Tarjeta Bancaria	Medio	<500

### Identificación del nivel de riesgo por tipo de dato.

Al definir el nivel de riesgo inherente por cada tipo de dato y el volumen de titulares, se podrá identificar el nivel de *riesgo por tipo de dato* que se trata en nuestra institución. Como se mencionaba supralíneas, se han establecido cinco niveles posibles con valor numérico del 1 al 5, donde **1** es el nivel **más bajo** y **5** el **más alto**, en este sentido, la esquematización del tipo de dato y tipo de riesgo gestionado en el INFOCOL, se describe de la siguiente manera:

#### TIPO DE DATO

#### RIESGO INHERENTE



De lo anterior, se precisa entonces, de acuerdo a la misma clasificación en la Metodología BAA, que el Riesgo por tipo de dato es de **Nivel 1**, el cual ocurre cuando:

- El nivel de riesgo inherente de los datos sea bajo, sin importar el número de personas.
- El nivel de riesgo inherente sea medio y se tengan hasta cinco mil (5,000) personas
- El nivel de riesgo inherente sea alto y se tengan hasta quinientas (500) personas

#### **FACTOR de Accesibilidad: El nivel de riesgo por tipo de acceso**

A este respecto, es necesario identificar el nivel de riesgo por tipo de acceso; el cual se realiza determinando la cantidad de accesos potenciales a los datos personales que se pretende proteger, definiendo cuántas personas tienen la posibilidad de acceder a la información en un intervalo de tiempo; para el caso de las instituciones públicas que son sujetos obligados en nuestro estado, como el INFOCOL, se puede tomar como referencia la jornada laboral de 8 horas. Para este parámetro, entre mayor sea la accesibilidad a las bases de datos que contengan datos personales por parte del personal de la institución o ajenos a la misma, mayor riesgo existe para dicha información; de ahí la importancia del diagnóstico inicial institucional, para determinar a través de la identificación de las bases de datos que resguardan datos personales y el control de inventario de los mismos, el personal que estará cargo de dicha responsabilidad de conformidad con los principios y deberes que nos marca la ley local en la materia.

Nivel de riesgo por tipo de acceso en el INFOCOL.

ACCESIBILIDAD	Número de personas que acceden a los Datos Personales	Cantidad de Acceso a los Datos Personales	Tipo de riesgo Inherente
	<10	<20	Mínimo

**FACTOR de Anonimidad: El nivel de riesgo por tipo de entorno.**

Después de obtener el factor **Accesibilidad**, se debe identificar qué tan anónimos son los accesos a la información; es decir, el nivel de *riesgo por tipo de entorno*. Este factor representa el nivel de percepción que se tiene de que un atacante potencial provoque consecuencias negativas para la institución, en caso de acceder o hacer uso no autorizado de los datos personales que se tratan.

En la siguiente tabla se listan los entornos de acceso, de igual forma en una escala del 1 al 5, en donde **1** implica **baja anonimidad** y **5** **mayor anonimidad** del atacante, es decir, entre más anónimo pueda ser un atacante, mayor confianza obtiene para intentar vulnerar la seguridad.

Nivel de riesgo por tipo de entorno en el INFOCOL.

ENTORNO	NIVEL DE ANONIMIDAD
FÍSICO	1 (Bajo)
RED INTERNA	1 (Medio)

## Identificación de medidas de seguridad

Una vez obtenido el nivel que le corresponde a cada factor de riesgo, se deben identificar las medidas de seguridad aplicables a la institución. Para ello, en la Metodología BAA se desarrollan cinco tablas matriciales que combinan el nivel de riesgo por tipo de dato, el nivel de accesibilidad y el nivel de anonimidad, dando como resultado un patrón de control o lista de controles a implantar. *(Para mayor información de las tablas matriciales de nivel 2, 3, 4 y 5 pueden consultar la Metodología completa BAA, enlace descrito en las fuentes consultadas al final del documento).*

### Tabla de control matricial para el INFOCOL.

Se utilizará lo correspondiente a la **Tabla 1**, que permita esquematizar la combinación del nivel de riesgo por tipo de dato, el nivel de accesibilidad y el nivel de anonimidad, que da como resultado identificar un patrón de control o lista de controles a implantar. Dicha tabla se utiliza solo por las instituciones públicas cuyo nivel de riesgo por tipo de dato **es 1**. Para todas las combinaciones de esta tabla le corresponde el **patrón de control de medidas básicas de seguridad (CB)**, mismo que deberá aplicarse en su totalidad y de manera específica a través de la análisis y selección de las medidas Físicas, Técnicas y Administrativas que aplican a dicho control de la seguridad de los datos personales.

		Riesgo por tipo de dato 1			
Entornos de acceso	Internet	CB			
	Red terceros				
	WiFi				
	Red interna				
	Físico				
		≤ 20	≤ 200	≤ 2,000	> 2,000
		Cantidad de Accesos/Personas			

A este respecto, antes de abordar el esquema que describe las medidas Físicas, Técnicas y Administrativas del INFOCOL, vale la pena realizar una concatenación funcional con la explicación y descripción de los elementos generales que contempla un análisis de brecha; el cual, junto con los elementos examinados y valorados en el análisis de riesgos, nos permiten explicar cuáles son las medidas de seguridad con las que cuenta actualmente el instituto, en que parámetro se realiza cada medida abordada, y en el caso de que aún no se realice, la meta temporal definida para su realización.

### **3.7 Medidas de seguridad y Análisis de Brecha**

Al igual que en el análisis de riesgos, el análisis de brecha se enfoca en la seguridad de los datos personales recabados y gestionados por cada área del INFOCOL que tenga las atribuciones y facultades para su tratamiento. Lo anterior, se hace realizando un diagnóstico de las prácticas de seguridad de la información con las que cuenta en ese momento el sujeto obligado y las que deberían de tenerse en un estado ideal de las cosas.

Toda vez que ya se ha exhaustivo un análisis de riesgos en nuestro Documento de Seguridad para la Protección de los Datos Personales, se resaltan a continuación los tópicos relevantes que confluyen y se concatenan con el mismo, en relación a un análisis de brecha, para continuar con la identificación y descripción de las medidas de seguridad Administrativas, Técnicas y Físicas con las que cuenta nuestra institución, así como también el parámetro de su implementación actual.

#### ***Seguridad institucional:***

*Control de la información compartida con terceros; a través de la identificación de los inventarios de datos personales por área, el responsable, y la aplicación de las medidas de seguridad para su protección.*

**Activos del responsable:**

*Entendiéndose por activo, el tipo de dato recabado y gestionado en la institución, de los cuales se asignan responsabilidades para su protección y clasificación.*

**Seguridad en recursos humanos:**

*Cuidar la seguridad de los recursos humanos previo a la contratación; cláusula contractual que comprometa y obligue al empleado a respetar el deber de seguridad y confidencialidad de los datos personales que gestiona.*

**Seguridad física y ambiental:**

*Áreas seguras y protección de equipamiento, especificadas en las medidas físicas para la protección de los datos personales.*

**Operación, procedimientos y comunicación:**

*Parte fundamental en desarrollo e implementación del Sistema de Gestión y el Programa de Protección de Datos Personales en su caso; herramientas que se pueden desprender del propio documento de seguridad, con el cual comparten elementos.*

**Cumplimiento con leyes y lineamientos:**

*Todas las herramientas y elementos de control propuestos están de conformidad a lo mandatado por la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, y lo conducente a nuestra ley local.*

**Control de acceso a la información:**

*Derechos y control de acceso a aplicaciones, redes y sistemas operativos al interior del instituto, especificados en las medidas técnicas de seguridad.*

**Incidentes de seguridad de información:**

*Se cuenta con los procedimientos y formatos establecidos para identificar y mitigar algún incidente de seguridad en la institución.*

En este tenor y tomando en cuenta el examen cuantitativo y cualitativo realizado a los tipos de datos recabados, detección de vulnerabilidades, niveles de riesgo y seguridad para la protección de los mismos, concatenado a estas directrices de

análisis planteadas como análisis de brecha, se presenta en el siguiente esquema, las medidas de seguridad en el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima (INFOCOL), el parámetro en que se realizan y la meta de su realización a corto plazo en el caso de las faltantes:

## Medidas de seguridad INFOCOL

### Medidas de Seguridad ADMINISTRATIVAS

Tipo de Medida de Seguridad	Mecanismo de Control	Parámetro en que se realiza
Administrativas	Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por el Pleno del Organismo Garante, publicada y comunicada a todos los empleados y terceras partes relevantes.	Los protocolos de capacitación, prevención y acciones en caso de vulneraciones a la seguridad de los datos personales aprobadas por el pleno del INFOCOL, y contenidas en este instrumento concentrador del documento de seguridad, se transmiten a todas las áreas involucradas en el manejo de datos personales, incluidas sus actualizaciones y modificaciones.



	Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	La Política de seguridad de la información es revisada y evaluada en periodos trimestrales.
	Atender las necesidades de seguridad cuando se trata con ciudadanos: Todos los requisitos identificados de seguridad deben atenderse antes de dar acceso a los ciudadanos, a los activos o información de la institución.	La Unidad de Transparencia y Acceso a la Información Pública del INFOCOL, como ventanilla de atención ciudadana, establece los parámetros de ley para asegurar los archivos y/o documentación cuando se solicite consulta directa a los mismos ante una solicitud de información pública.
	Inventario de activos: Todos los activos deben ser claramente identificados y se debe elaborar y mantener un inventario de los activos más importantes.	Se tiene un inventario de datos personales por cada área en el Instituto involucrada en el manejo y tratamiento de datos personales.

	<p>Roles y responsabilidades: Los roles y responsabilidades de seguridad de los empleados deben estar definidos y documentados en concordancia con la política de seguridad de la información de la institución.</p>	<p>El sistema de gestión para las medidas de seguridad contenido en este documento de seguridad contiene las especificaciones respecto a los roles y responsabilidades del personal involucrado en el tratamiento de datos personales.</p>
	<p>Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.</p>	<p>De conformidad con el artículo 44 de la LPDPPSOEC, en lo concerniente al deber de confidencialidad; todo el personal encargado de la gestión y tratamiento de datos personales al interior del instituto, tiene en su expediente laboral, una carta compromiso de confidencialidad firmada, como parte de los requisitos de ingreso.</p>

	<p>Concienciación, educación y entrenamiento de seguridad de la información: Todos los empleados de la institución deben recibir concienciación. Asimismo debe darse entrenamiento de forma periódica en las políticas y procedimientos organizacionales, conforme a la importancia de su función en el trabajo.</p>	<p>La información y el entrenamiento correspondiente al desempeño institucional y la gestión de la seguridad de los datos personales, está contenida en el plan anual de capacitación en esta materia.</p>
	<p>Administración de medios removibles: Deberán documentarse e implementarse procedimientos para la gestión de medios removibles.</p>	<p>Todo componente extraíble de hardware que sea usado para el almacenamiento de información; está sujeto a los Procedimientos de respaldo y recuperación de datos personales, y en su caso a las Técnicas de Supresión y Borrado Seguro de Datos Personales contenidas en este documento de seguridad.</p>
	<p>Deberán establecerse acuerdos para el intercambio de información y aplicaciones entre el instituto y las entidades externas.</p>	<p>Para ello, se estará a lo estipulado en el Título Quinto, Capítulo Único de la LPDPPSOEC.</p>

	Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Actividades planteadas y descritas en el Sistema de Gestión para las medidas de seguridad incluidas en el documento concentrador de seguridad.
	Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Procedimiento formal descrito en el Sistema de Gestión para las medidas de seguridad incluidas en el documento concentrador de seguridad.
	Procedimientos de control de cambios: La implementación de los cambios debe ser controlada mediante el uso de procedimientos formales de control de cambios.	La planificación trimestral para el monitoreo y revisión las medidas de seguridad y el sistema de gestión para la protección de los datos personales permite tener un control de cambios y actualizaciones.
	Se deben establecer procedimientos y responsabilidades de la administración para asegurar una adecuada, ordenada y oportuna respuesta a los incidentes de seguridad	Dichos procedimientos y responsabilidades, están plasmados en el plan de respuesta para incidentes de seguridad de la información y los datos personales.

	Verificación del cumplimiento técnico: Se deben verificar constantemente los sistemas de información para el cumplimiento de los estándares de seguridad.	La planificación trimestral para el monitoreo y revisión las medidas de seguridad y el sistema de gestión para la protección de los datos personales permite tener un control de cambios y actualizaciones.
	Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	El establecimiento de roles y responsabilidades del personal y las áreas encargadas del tratamiento de datos personales, se encuentran definidas en el formato de base de datos, dentro del Sistema de Gestión para las medidas de seguridad.
	Retorno de los activos: Todos los empleados deben regresar a la institución todos los activos que tengan en posesión una vez se termine el trabajo, contrato o acuerdo.	Lo anterior se encuentra plenamente estipulado en el reglamento Interior de este Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima.

## Medidas de Seguridad TÉCNICAS

Tipo de Medida de Seguridad	Mecanismo de Control	Parámetro en que se realiza
Técnicas (Seguridad de la Red Interna)	Eliminación o reutilización segura del equipo: Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre-escritura apropiada de cualquier información sensible y "software" de autor antes de su eliminación	Todo medio de almacenamiento o equipo de cómputo, después de pasar por el procedimiento administrativo de baja del inventario, se canaliza a la Secretaría de Informática para análisis y resguardo.
	Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Se estableció una planeación con base en revisiones y auditorías semestrales de la calidad y funcionamiento de los antivirus y protecciones con los que cuentan los equipos.
	Controles de red: Las redes deben ser gestionadas y controladas con el fin de ser protegidas de las amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.	El servidor y red interna es monitoreado permanentemente para detectar posibles amenazas o fallas por causas fortuitas.

	<p>Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.</p>	<p>Se llevan a cabo bitácoras y registros de auditoría trimestrales en relación a los usuarios de los equipos donde se resguarden y gestionen datos personales.</p>
	<p>Administración de privilegios: Deberá restringirse y controlarse la asignación y uso de privilegios.</p>	<p>La administración del control y asignación de privilegios viene definida de raíz desde la identificación y descripción del formato de base de datos, mismas que se integran al Sistema de Gestión.</p>
	<p>Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.</p>	<p>Se cuenta con el listado de privilegios y contraseñas por usuario de equipo de cómputo y se realiza sensibilización del adecuado cuidado y uso de las mismas.</p>

	Equipos desatendidos: Los usuarios deberán asegurar que los equipos atendidos cuenten con protección adecuada.	Los equipos de cómputo cuentan con antivirus especializado y actualizado para prevenir amenazas externas.
	Identificación y autenticación de usuarios: Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	Cada trabajador de área ejecutiva y administrativa, cuenta con un equipo de cómputo a su resguardo, el cual cuenta con ID de usuario por cada usuario, para garantizar la identidad de quien gestiona la información en el equipo.
	Control de vulnerabilidades técnicas: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan. Se debe evaluar la exposición de la institución a las mismas y se deben tomar las medidas apropiadas para enfrentar los riesgos asociados.	Dicho análisis y especificaciones técnicas y de acción, se encuentran contenidos en el plan de respuesta para incidentes de seguridad de la información y los datos personales.



	<p>RespalDOS de información:</p> <p>Deberán realizarse copias de respaldo de la información y aplicaciones. Se deberán probar los respaldos de acuerdo a una política establecida.</p>	<p>Las áreas competentes para el tratamiento de datos personales en el INFOCOL, realizan de manera mensual un respaldo de la información contenida en su equipo de cómputo. Dicho esquema se encuentra regulado en el Sistema de Gestión para la seguridad de los datos personales.</p>
--	--	---

### Medidas de Seguridad FÍSICAS

Tipo de Medida de Seguridad	Mecanismo de Control	Parámetro en que se realiza
Físicas	Control de ingreso a las instalaciones y diferentes áreas ejecutivas y administrativas del instituto.	El ingreso de los empleados se encuentra supeditado al control de asistencia por huella digital, que es un sistema que gestiona la información de horarios de entrada y salida de los empleados; a su vez, cada responsable de área, tiene la responsiva de mantener bajo llave su sitio de trabajo diario al desocuparse del mismo.

	<p>Los derechos de acceso de todos los empleados a la información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.</p>	<p>Junto con la entrega recepción del empleado en un área determinada al finalizar su relación laboral con el instituto, se inicia el protocolo de revocación de los derechos de acceso a la información, equipos y procedimientos del INFOCOL.</p>
	<p>Perímetro de seguridad física: Los perímetros de seguridad (barreras, tales como paredes, tarjetas que controlan entradas o recepciones) deben ser implementados para proteger áreas que contienen información y sistemas de información.</p>	<p>Se ha implementado en la recepción del INFOCOL, una puerta intermedia de acceso a las instalaciones, con el objetivo de que la Unidad de Transparencia controle el tránsito y los ingresos al instituto mediante protocolos específicos.</p>
	<p>Eliminación y entrega de los medios de almacenamiento: Los medios deberán eliminarse de modo seguro cuando no se les necesite más, usando procedimientos formales.</p>	<p>Una vez que se ha sido exhaustivo con las técnicas de supresión y borrado Seguro, los dispositivos físicos de almacenamiento y respaldos de información, se desechan y destruyen mediante procedimientos seguros.</p>

	Medios físicos de almacenamiento en tránsito: Cualquier medio que contenga información deberá ser protegido contra acceso no autorizado, mal uso o corrupción durante su transporte más allá de los límites de la institución.	Por reglamento interno de la institución, no se tienen autorizaciones o privilegios para transportar equipos de cómputo o medios de almacenamiento fuera de los límites del Instituto.
	Seguridad de los espacios, ventanales y las bardas perimetrales.	Se asegura de que los ventanales de las diferentes áreas sean herméticos para evitar la entrada de polvo y agua de lluvia; a su vez, se le da mantenimiento a las paredes perimetrales de cada área una vez al año, detectando y previniendo humedad y salitre en las mismas.
	Cuidado, mantenimiento y renovación del mobiliario de oficina.	Cajas de archivo, archiveros, escritorios y cajones de aglomerado o MDF, anaqueles de metal, se encuentran estratégicamente acomodados en cada sección y área del instituto, para evitar daños por golpes o humedad.

	<p>Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.</p>	<p>Se lleva a cabo sin una periodicidad o planeación establecida; aspecto que se esquematizará mediante una planeación de auditorías y seguimiento anual.</p>
	<p>Protección del equipo: El equipo debe estar situado y protegido para reducir los riesgos de amenazas y peligros ambientales, y oportunidades de acceso no autorizado.</p>	<p>Los espacios del edificio tienen constante mantenimiento de pintura e impermeabilización, los equipos están situados estratégicamente en espacios con alarma y vigilancia interna.</p>
	<p>Seguridad de los equipos en el exterior: La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la institución.</p>	<p>Por reglamento interno solo en casos excepcionales de emergencia, se podrá sacar equipo o medios de almacenamiento para trabajar desde casa.</p>

## Segunda Fase

### 3.8 Implementación y Operación del SGSDP

Una vez realizados los análisis correspondientes para determinar los tipos de datos personales que gestiona la institución, e identificadas las medidas de seguridad con las que cuenta se cuenta y el parámetro en que se realiza; se llega la fase de echar a andar el plan de acción; la implementación y la operación de las políticas, procesos, procedimientos y controles o mecanismos del Sistema de Gestión de Seguridad de los Datos Personales (SGSDP) al interior del INFOCOL. En el caso que nos ocupa, en esta fase se deberán implementar las medidas de seguridad que hayan resultado aplicables según el análisis de riesgos realizado en la fase de planeación.

Se deberán considerar un conjunto de indicadores para identificar de manera oportuna, cualquier cambio en el contexto de nuestra institución y así mantener una visión general de la imagen del riesgo, entre más pronto se realice esta detección, las partes interesadas podrán tomar decisiones más efectivas para proteger los datos personales. La naturaleza de los indicadores puede variar dependiendo del tipo de activo, por ejemplo:

- Vigilar la actitud de un empleado inconforme con la institución.
- Cuidar que no se dejen documentos con información personal en las impresoras o fotocopadoras.
- Vigilar que el personal cumpla con la normativa interna en relación al manejo de documentos, y no los saque arbitrariamente de la institución.
- Indicadores relacionados con la capacitación constante del personal.
- E indicadores realacionados con los resultados de auditorias al funcionamiento del propio sistema.

El monitoreo de estos indicadores conllevan una detección temprana de posibles amenazas, y así lograr una respuesta a incidentes efectiva.

### **3.9 Implementación de las Medidas de Seguridad Aplicables a los Datos Personales**

Para realizar con éxito todas las actividades concernientes a la implementación del SGSDP, debe designarse un miembro del equipo del responsable para la rendición de cuentas de la gestión de los datos personales dentro de la institución, de modo que tanto el cumplimiento a la legislación en protección de datos, como a la política de gestión y seguridad de datos personales puedan ser demostrados. En el caso del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Colima, el servidor público responsable es el siguiente:

Mtro. Juan Carlos González Torres  
Secretario de Protección de Datos Personales  
Del INFOCOL  
[jgonzalez@infocol.org.mx](mailto:jgonzalez@infocol.org.mx)

El cual, tiene a su cargo las siguientes responsabilidades:

- a) Compromiso total del cumplimiento de la política;
- b) Desarrollo y revisión de la política;
- c) Asegurar la implementación de la política;
- d) Revisiones de la gestión de la política;
- e) Entrenamiento y concienciación necesaria de la política;
- f) Aprobación de procedimientos donde sean tratados los datos personales, como:
  - Administración interna de datos personales de los trabajadores que laboran en la institución.
  - El manejo de solicitudes de información y de datos personales por la Unidad de Transparencia y áreas competentes.

- La recolección, manipulación y resguardo de datos personales derivado de asesorías ciudadanas en el ejercicio de Acceso a la Información pública y Datos Personales, de las áreas que brindan atención al público.
- Manejo y reguardo de datos personales en la gestión de medios de impugnación, quejas ciudadanas (Recurso de Revisión).
- La gestión de los datos personales en la detección de posibles riesgos a la seguridad de los datos o incidentes de seguridad;
- Protocolos de actuación ante una inminente vulneración a la seguridad de los datos personales en la institución.

g) Enlace con las personas a cargo del manejo de riesgos y asuntos de seguridad dentro de la institución;

h) Provisión de asesoramiento en asuntos ante el INAI y en relación con proyectos que involucren temas de seguridad de los datos personales, como puede ser compartirlos o transferirlos fuera de la institución;

i) Interpretación de las exenciones aplicables al tratamiento de los datos personales;

j) Asegurar que la institución tenga acceso a actualizaciones legislativas y a una orientación apropiada de acuerdo a la legislación en protección de datos;

k) Revisar que el SGSDP refleje los cambios en legislación, práctica y tecnología a través una comunicación continua y proactiva del riesgo a las partes interesadas;

l) Completar, emitir, y gestionar notificaciones ante el INAI y los titulares de datos personales cuando sea requerido según la normatividad aplicable; y

m) En su caso, implementar las prácticas relacionadas al tratamiento de datos personales enmarcadas en cualquier normativa de sector público que aplique a nuestra institución.

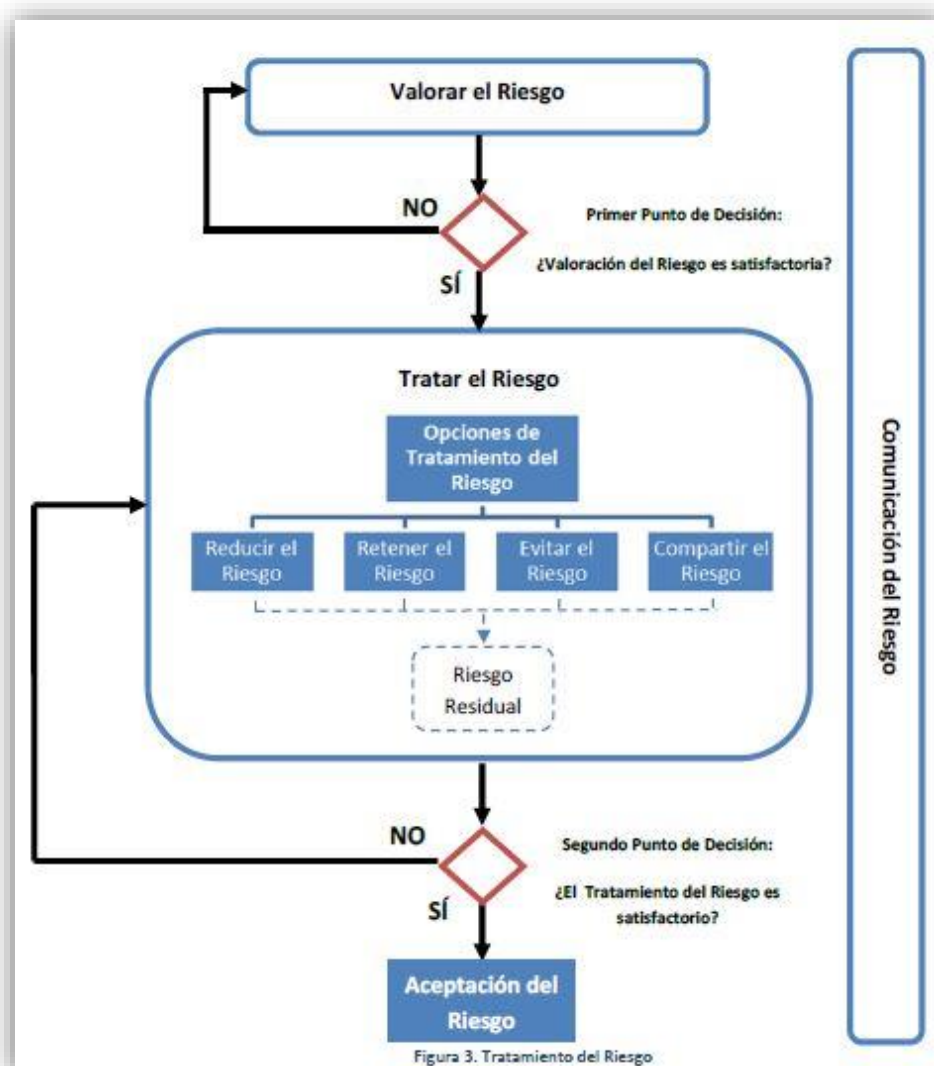
Cuando la institución posea múltiples departamentos o sistemas que procesan información personal, debería determinar si es apropiado establecer una red de representantes en protección de datos personales, los cuales:

- a) Representen departamentos o sistemas que sean reconocidos como relevantes, ya sea por el tipo de proceso o por el tipo de dato personal que manejan en relación con la gestión de información; y
- b) Ayudar a los trabajadores con las responsabilidades diarias para el cumplimiento de la política.



### 3.10 Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes.

En necesario planear y señalar las acciones que se tomarán en cuenta para mantener actualizadas las medidas de seguridad físicas, técnicas y administrativas que identificamos y analizamos en el análisis de riesgo y de brecha, describiendo la forma en que se llevarán a cabo dichas acciones y la temporalidad que tendrán. Existen cuatro posibilidades comunes para tratar el riesgo: mitigar o reducir el riesgo, retener el riesgo, evitar el riesgo y compartir el riesgo. La Figura 3 ilustra el tratamiento del riesgo dentro del proceso de un SGSDP.



Las opciones de tratamiento del riesgo se seleccionan con base en el resultado de la valoración del riesgo, los costos estimados, y los beneficios esperados de implementar estas opciones. Si se obtiene una considerable reducción del riesgo con un costo relativamente bajo, esto es una combinación a considerar para implementar los controles. En general, las consecuencias adversas de los riesgos deben reducirse lo más razonablemente posible con independencia de cualquier criterio absoluto, por ejemplo, se deben considerar los riesgos que no ocurren con frecuencia pero que serían severos, en cuyo caso también se deben implementar controles y aterrizar parámetros de acción concretos para corregir e implementar lo faltante en nuestra institución con respecto a las medidas de seguridad.

Los cuatro tipos de tratamiento de riesgo descritos en la figura 3 supralíneas, no son mutuamente excluyentes, a veces las instituciones pueden beneficiarse sustancialmente de la combinación de opciones, como reducir la probabilidad de un riesgo, reducir sus consecuencias, compartir o retener el riesgo residual, el cual hace referencia a aquel riesgo que permanece después de que el titular de la institución o el equipo de respuesta a incidentes de seguridad desarrolle sus respuestas a los riesgos. El riesgo residual pues, refleja el riesgo remanente una vez se han implantado de manera eficaz las acciones planificadas para mitigar el riesgo inherente.

Continuando con el punto, una vez definido nuestro plan de acción, se requiere determinar el riesgo residual. Si el riesgo residual no cubre los niveles de aceptación de la institución, se deberá realizar otra iteración de tratamiento del riesgo antes de proceder a la aceptación del riesgo. Finalmente se deben implementar los controles correspondientes así como documentar todas las acciones derivadas de la planeación e implementación del tratamiento del riesgo.

## Opciones de Tratamiento de Riesgo.

### ***Reducir el Riesgo***

El objetivo es seleccionar los controles apropiados y justificados para satisfacer los requerimientos especificados por la valoración del riesgo. Los controles pueden proporcionar uno o más de los siguientes tipos de protección:

- ✓ Corrección
- ✓ Eliminación
- ✓ Prevención
- ✓ Minimización del impacto
- ✓ Disuasión
- ✓ Recuperación
- ✓ Monitoreo
- ✓ Concienciación.

Durante la selección de controles es importante ponderar el costo de adquisición, implementación, administración, operación, monitoreo y mantenimiento de los controles contra el valor del activo a proteger. Adicionalmente, se debe tener en consideración el conocimiento y habilidades especiales necesarias para definir e implementar nuevos controles o modificar los existentes.

Existen factores que pueden afectar la selección de controles. Límites técnicos, como requerimientos de rendimiento, capacidad de gestión (soporte operacional necesario) y los asuntos de compatibilidad, pueden obstaculizar el uso de ciertos controles o pueden inducir a errores humanos nulificando el control, dando un falso sentido de seguridad o incrementando el riesgo más allá del control, por ejemplo, exigir contraseñas complejas sin previo entrenamiento, llevando a los usuarios a escribir las contraseñas en papel. Los responsables deben identificar las soluciones que satisfagan sus requerimientos y que garanticen suficiente seguridad de los datos personales.

### ***Retener el Riesgo.***

Se puede tomar la decisión de retener el riesgo sin considerar medidas adicionales si a través de la evaluación del riesgo se determina que no hay necesidad inmediata de implementar controles adicionales o que estos controles se pueden implementar posteriormente. Por ejemplo, el equipo de cómputo actual falla, pero se genera un respaldo de esa información al final del día, por lo que se decide retener ese riesgo durante un mes y esperar para cambiar el equipo de cómputo por uno nuevo.

### ***Evitar el Riesgo.***

Cuando el riesgo identificado es muy alto o los costos de tratamiento exceden a los beneficios, se debe tomar una decisión para evitar el riesgo, retirándose de las actividades actuales o cambiando las condiciones bajo las cuales operan dichas actividades. Por ejemplo, para un riesgo causado por la naturaleza podría ser más eficiente en costo mover físicamente el site de datos a una ubicación donde no exista el mismo riesgo o que se pueda mantener bajo control.

### ***Compartir el Riesgo.***

Implica tomar la decisión de compartir el riesgo con un prestador de servicio que pueda gestionarlo, es decir, un tercero interviene para mitigar los posibles efectos de un riesgo por ejemplo, al contratar un seguro o un proveedor que administre la seguridad de la institución. Cabe mencionar que cuando una institución comparte un riesgo no deja de ser responsable por la protección de los datos personales, además, es importante que se considere que involucrar a un nuevo actor en los procesos de la institución siempre representa un riesgo que debe ser analizado; lo anterior, aunado a que generalmente en el caso de la Administración Pública Estatal, no se cuenta con recursos financieros suficientes para hacer contrataciones externas de este tipo de servicios, se hace muy poco probable tomar en cuenta este tipo de estrategia.

### ***Aceptación del Riesgo Residual.***

Al llegar al punto de aceptar el riesgo se deben asumir y registrar formalmente las decisiones sobre el plan de tratamiento del riesgo, así como el riesgo residual, el plan de tratamiento del riesgo debe describir cómo se tratarán los riesgos valorados para alcanzar los niveles de aceptación. Es importante que el titular de la dependencia pública, apruebe y revise tanto los planes de tratamiento, como el riesgo residual. Del mismo modo, deberá registrarse cualquier condición asociada con tal aprobación.

Aceptar el riesgo implica que el riesgo residual no entre en conflicto con los criterios previamente establecidos en los objetivos y alcances de la institución, por ejemplo, el riesgo residual no puede considerar la aceptación de un riesgo relacionado al cumplimiento de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Colima (LPDPPSOEC), si esta forma parte de las metas planteadas nuestro Sistema de Gestión.

### ***Comunicación del Riesgo.***

Comunicar el riesgo es la actividad que resulta de alcanzar los acuerdos sobre el cómo administrar los riesgos, considerando su naturaleza, forma, probabilidad, severidad, tratamiento y aceptación. La comunicación efectiva entre los involucrados es muy importante pues impacta en las decisiones que se deban tomar, de ahí que tendría que ser bidireccional para asegurar que los involucrados en la implementación del Sistema de Gestión (SGSDP) y las partes interesadas entiendan los criterios en los que se basan las decisiones. A este respecto, en nuestro documento de seguridad ya se han definido los contactos prioritarios que entrarán en acción en el caso de detección de un riesgo o incidente de seguridad.

Como sabemos, la comunicación del riesgo se debe realizar para alcanzar los siguientes objetivos:

- ✓ Ofrecer garantías sobre la gestión del riesgo.
- ✓ Recolectar información sobre el riesgo.

- ✓ Compartir los resultados de la valoración y el plan de tratamiento del riesgo.
- ✓ Evitar o reducir las vulneraciones de seguridad por desconocimiento entre los involucrados en el SGSDP.
- ✓ Dar soporte a la toma de decisiones.
- ✓ Obtener nuevo conocimiento sobre la seguridad de la información.
- ✓ Que los responsables de datos personales coordinen con los encargados y terceros, los planes de respuesta en caso de una vulneración.
- ✓ Dar a los a los custodios y a las partes interesadas sentido de responsabilidad sobre el riesgo.
- ✓ Incrementar la conciencia del riesgo en nuestra institución.

Para este punto, es que se desarrollan los planes de comunicación del riesgo para las operaciones normales, así como para casos de emergencia, es decir, la comunicación del riesgo es una actividad continua. Es importante mantener la comunicación entre las áreas y servidores públicos afines a la difusión y el Oficial de Protección de Datos Personales para responder por ejemplo, a los ciudadanos en caso de incidentes de seguridad a sus datos personales.

Una vez descrito lo anterior, en relación a las diferentes acciones que se pueden tomar para intervenir ante un riesgo, se hace necesario esquematizar mediante controles y parámetros de realización conforme a los elementos faltantes detectados en el listado de las medidas de seguridad implementadas en el INFOCOL, la detección, valoración y prevención de posibles riesgos; para lo cual se implementa nuestro Plan de Trabajo, señalando como control la medida de seguridad faltante, y como parámetro, la acción que se realizará para subsanarlo al corto o mediano plazo.

## Medidas de Seguridad ADMINISTRATIVAS

CONTROL	PARÁMETRO DE REALIZACIÓN
Documentación de la política de seguridad de la información: La política de seguridad de la información debe ser aprobada por el Pleno del Organismo Garante, publicada y comunicada a todos los empleados y terceras partes relevantes.	Los instrumentos normativos como el Documento de seguridad, Sistema de Gestión para la protección de los datos personales y el Programa anual de Protección de Datos Personales serán aprobados cada primero de abril del ejercicio en curso.
Revisión de la Política de seguridad de la información: La política de seguridad de la información debe ser revisada en intervalos planeados o si ocurren cambios significativos, para asegurar su continua aplicabilidad, adecuación y efectividad.	Se realizará una valoración trimestral de la vigencia y actualidad de la política de seguridad de la información, misma que se traduce en el monitoreo los cambios y la vigencia de los instrumentos normativos desarrollados para la gestión y seguridad de los datos personales.
Términos y condiciones de empleo: Como parte de su obligación contractual, los empleados deben acordar y firmar los términos y condiciones de su contrato de empleo, el cual debe indicar su responsabilidad respecto a seguridad de la información.	Se establecerá como parte del expediente único que la Secretaría de Administración recaba de cada trabajador al momento de su contratación, la obligatoriedad contractual de comprometerse a resguardar y proteger la información que gestiona, así como también firmar carta de confidencialidad en relación al tratamiento de datos personales ordinarios y sensibles.

Uso Sistema de monitoreo: Se deben establecer procedimientos para monitorear el uso de la información y los sistemas. Los resultados de las actividades de monitoreo deben ser revisados con regularidad.	Diseñar reportes y bitácoras trimestrales de revisión de la información que se gestiona por cada una de las áreas que dan tratamiento a datos personales, así como los sistemas en que se soportan, para la detección de posibles vulneraciones o riesgos.
Registro de usuarios: Deberá existir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.	Que la totalidad del personal que gestiona información en equipo y soporte electrónico, tenga un usuario y contraseña debidamente registrado.
Distribución de las responsabilidades de seguridad de la información: Todas las responsabilidades de seguridad deben estar claramente definidas.	Junto con el personal que conforma el equipo de atención a incidentes de seguridad de la información, se crearan políticas definidas de intervención y reacción por parte de todo el personal.

## Medidas de Seguridad TÉCNICAS

CONTROL	PARÁMETRO DE REALIZACIÓN
Se deberán implementar controles para la detección, prevención y recuperación de la infraestructura en contra de códigos maliciosos. Se deberán implementar procedimientos de concienciación adecuados.	Se lleva a cabo de manera periódica la revisión y actualización de los antivirus que protegen los equipos, sin embargo es necesario fortalecer los procedimientos internos de capacitación y concienciación del personal.



Registro de auditoría: Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.	No se realiza actualmente. Dadas las características del Software y los equipos de cómputo que conllevan en si riesgos de vulneraciones físicas y electrónicas; se realizará una auditoría anual a las actividades de los usuarios, las excepciones, y eventos de seguridad que se hayan suscitado.
Uso de contraseñas: Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.	El área auditora, establecerá dentro de las supervisiones, que el total del personal que maneja equipo de cómputo se suscriba a la práctica de seguridad mediante uso de contraseña.
Todos los usuarios deben tener un identificador único (ID de usuario) para su uso personal, y una técnica de autenticación adecuada debe ser elegido para fundamentar la identidad declarada de un usuario.	Derivado de un reciente cambio de inventario de bienes muebles, hay personal que aún no cuenta con ID de identificación en su equipo de cómputo, lo cual atenderá.

## Medidas de Seguridad FÍSICAS

CONTROL	PARÁMETRO DE REALIZACIÓN
Los derechos de acceso de todos los empleados a la información e instalaciones de procesamiento de información deben ser removidos en cuanto se termine el trabajo, contrato, acuerdo o cuando se requiera hacer un ajuste.	Al momento de su contratación, el trabajador adquiere la obligatoriedad contractual de realizar entrega recepción del cargo que finaliza, lo cual implica todo lo relacionado a privilegios otorgados para el manejo de Software y Hardware institucionales.

<p>Seguridad de los espacios, ventanales y las bardas perimetrales.</p>	<p>Se llevan a cabo mantenimientos y renovaciones solo cuando ya es evidente un daño material. Por lo cual se establecerá un diagnóstico semestral por parte del personal de Administración para mantenimiento de los espacios.</p>
<p>Se deberán producir y almacenar registros de auditoría relacionados a las actividades de los usuarios, las excepciones, y eventos de seguridad. Estos registros deberán ser utilizados en futuras investigaciones y monitoreo de control de accesos.</p>	<p>Dadas las características físicas de los equipos de cómputo, archiveros y anaqueles metálicos, que conllevan en si riesgos de deterioro físico; el diagnóstico de mantenimiento, será parte de una auditoría anual a las instalaciones en relación a los bienes muebles mencionados.</p>
<p>La seguridad debe ser aplicada en equipos en el exterior tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la institución.</p>	<p>Por normatividad interna, no se puede sacar activos ni equipo de las instalaciones; sin embargo para situaciones emergentes de desarrollará normatividad interna al respecto.</p>

## Tercera Fase

### 3.11 Monitoreo y Revisión del SGSDP

En esta fase, como se señaló anteriormente, se evalúan y miden los resultados de las políticas, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.

### 3.12 Revisiones y Auditoría

#### ***Revisión de los Factores de Riesgo.***

Se debe monitorear y revisar el riesgo con sus factores relacionados, es decir, el valor de los activos, que para nuestro caso como entidades públicas, los activos son precisamente los datos personales ordinarios o sensibles que se recaban, así como los sistemas de tratamiento en que se encuentran contenidos, junto con las amenazas, vulnerabilidades, el impacto, y la probabilidad de ocurrencia, para identificar en una etapa temprana cualquier cambio en el contexto del alcance y objetivos del SGSDP de nuestra institución y así mantener una visión general de la imagen del riesgo.

***El riesgo no es estadístico:*** las amenazas, vulnerabilidades, probabilidad y consecuencias pueden cambiar abruptamente sin previo aviso. Esta situación exige la revisión de cada riesgo por separado, así como la suma de ellos, para conocer el impacto potencial acumulado de las amenazas. Por lo tanto, se requiere de constante monitoreo para detectar esos cambios; asegurarnos que los siguientes puntos estén continuamente monitoreados:

- ✓ Nuevos activos que se incluyan en los alcances de la gestión de riesgo.
- ✓ Modificaciones necesarias a los activos, por ejemplo, cambio o migración tecnológica.
- ✓ Nuevas amenazas que podrían estar activas dentro y fuera de la institución y que no han sido valoradas.

- ✓ La posibilidad de que vulnerabilidades nuevas o incrementadas sean explotadas por las amenazas correspondientes.
- ✓ Vulnerabilidades identificadas para determinar aquéllas expuestas a amenazas nuevas o pasadas que vuelven a surgir.
- ✓ Cambio en el impacto o consecuencias de amenazas valoradas, vulnerabilidades y riesgos en conjunto, que resulten en un nivel inaceptable de riesgo.
- ✓ Incidentes y vulneraciones de seguridad.

El resultado del monitoreo de riesgo puede afectar su tratamiento y aceptación, y en consecuencia el contexto que se establezca en la siguiente iteración del ciclo del SGSDP de nuestra institución.

### ***Auditoría.***

Se debe contar con un programa de auditoría interna para monitorear y revisar la eficacia y eficiencia del SGSDP. Este programa debe planearse, establecerse y mantenerse tomando en cuenta la política de gestión de datos personales. Se deben establecer previamente los objetivos del programa de auditoría, el cual debe incluir el alcance e indicar explícitamente cualquier tratamiento de datos personales interno y externo a la institución, responsables, recursos, criterios a utilizar durante la auditoría, así como los procesos y/o áreas que serán auditadas.

La objetividad e imparcialidad del programa de auditoría debe ser asegurado por la apropiada selección de auditores y la conducción de la auditoría. Las auditorías deben llevarse a cabo en intervalos de tiempo planeados para determinar si el SGSDP:

- a) está operando de acuerdo con la política de gestión de datos personales y con los procedimientos establecidos, y
- b) ha sido implementado y mantenido de acuerdo con los requerimientos tecnológicos.

Se debe proporcionar al titular de nuestra institución los reportes de las auditorías sobre el SGSDP, detallando cualquier desviación significativa de la política de gestión de datos personales, como pueden ser asuntos relacionados con los procesos de seguridad que puedan afectar su cumplimiento.

La auditoría debe ofrecer al responsable información detallada respecto a cambios ocurridos en el SGSDP, además se debe realizar una auditoría inmediatamente después de la implementación de modificaciones mayores en el SGSDP o en los procesos críticos de la institución respecto al tratamiento de datos personales. Como resultado de una auditoría se deben obtener observaciones sobre riesgos existentes para aplicar medidas preventivas, es decir, controles para que no ocurra una vulneración, así como observaciones sobre puntos que requieren medidas correctivas inmediatas.

Las revisiones y auditorías, así como diferentes indicadores y alertas en el SGSDP pueden avisar la ocurrencia de vulneraciones a la seguridad de los datos personales en cualquier fase del tratamiento. La institución debe contar con procedimientos para tomar acciones que permitan el manejo de las vulneraciones de seguridad que puedan ocurrir, considerando al menos:

#### **1.- Identificación de la vulneración.**

En caso de un incidente de seguridad, la institución debe identificar:

- a. Los activos afectados junto con el personal a cargo.
- b. Los titulares afectados.
- c. Partes interesadas que requieran estar informadas y/o puedan tomar parte en la toma de decisiones para mitigar las consecuencias de la vulneración.

**2.- Notificación de la vulneración.** Una vez identificada la vulneración, ésta se debe comunicar a los titulares de los datos personales para que puedan tomar medidas que mitiguen o eviten una posible afectación. Dependiendo del riesgo que implique para los titulares, la notificación de una vulneración puede ser a través de medios de comunicación masivos como un anuncio en su página web, periódico, radio o bien, de manera personalizada. Dependiendo de la gravedad del asunto, se podría incluso considerar notificar a las autoridades de justicia en la materia, entre otras partes interesadas que pudieran auxiliar en el proceso de mitigar el incidente. Además de la información pertinente sobre la vulneración, como puede ser la naturaleza del incidente y los datos personales comprometidos, se debe notificar de las acciones inmediatas que está tomando nuestra institución, así como proporcionar mecanismos de atención para que los titulares estén informados y reciban recomendaciones para reducir su afectación.

**3.- Remediación del incidente.** Una vez identificada la vulneración y después de haber realizado la respectiva notificación, se debe profundizar en el análisis de las causas del incidente para establecer medidas correctivas, las cuales incluyen medidas inmediatas para reducir los efectos de la vulneración, así como medidas a largo plazo por ejemplo, implementar controles técnicos o actualizar las políticas del SGSDP para evitar que incidentes similares o relacionados vuelvan a ocurrir.

Las revisiones, auditorías y los tratamientos de una vulneración a la seguridad al SGSDP deben estar debidamente documentados, incluyendo un resumen de los hallazgos y los planes para aplicar medidas preventivas y correctivas con objeto de que el equipo encargado, cuente con evidencia suficiente para mostrar al Organismo Garante en su caso, su diligencia en tomar las acciones necesarias para evitar o mitigar una vulneración a la seguridad de los datos personales, además de que estos procesos proporcionan información que sirve como entrada para los procesos de mejora continua del SGSDP.

## Cuarta Fase

### 3.13 Mejorar el SGSDP

El monitoreo de los factores de riesgo así como los resultados de las auditorías proporcionan información para demostrar la eficacia del SGSDP, pero también presentan las áreas de oportunidad donde éste puede ser mejorado.

**Los puntos de mejora del SGSDP pueden corresponder a dos tipos:**

a) **Acciones correctivas.**

Son las acciones encaminadas a eliminar las causas de fallas o incidentes **ocurridos** en el SGSDP, con objeto de prevenir que vuelvan a ocurrir, dichas acciones deben ser proporcionales a la gravedad del incidente. Las acciones correctivas deben atenderse considerando:

- i. El análisis y revisión de la falla o incidente;
- ii. Determinar las causas que dieron origen a la falla o incidente;
- iii. Evaluar las acciones necesarias para evitar que la falla o incidente vuelva a ocurrir;
- iv. Determinar e implementar las acciones necesarias;
- v. Registrar los resultados de las acciones tomadas;
- vi. Revisar la eficacia de las acciones correctivas tomadas.

b) **Acciones preventivas.**

Son las acciones encaminadas a eliminar las causas de fallas o incidentes **posibles** en el SGSDP, dichas acciones deben ser proporcionales a las amenazas potenciales. Las acciones preventivas deben atenderse considerando:

- i. El análisis y revisión de la amenaza;
- ii. Determinar las fallas o incidentes que podría desencadenarse con una amenaza;
- iii. Evaluar las acciones necesarias para evitar que la falla o incidente ocurra;

- iv. Determinar e implementar las acciones necesarias;
- v. Registrar los resultados de las acciones tomadas;
- vi. Revisar la eficacia de las acciones preventivas tomadas.

La implementación de las acciones preventivas o correctivas puede establecerse en un periodo inmediato a la detección y análisis del punto de mejora (por ejemplo, en respuesta a los resultados de una auditoría) o calendarizarse para una futura revisión del SGSDP en función de la importancia de la mejora y los recursos disponibles. La eficacia de las acciones preventivas y correctivas se evalúa considerando la reducción de los niveles de riesgo en los resultados del monitoreo a los SGSDP o de auditorías posteriores. En función de las acciones correctivas y preventivas, así como de la actualización del contexto de la organización resultado del monitoreo del riesgo, se deben establecer o mejorar los planes de capacitación.

### 3.14 Mejora Continua y Capacitación

La mejor medida de seguridad contra posibles vulneraciones es contar con personal consciente de sus responsabilidades y deberes respecto a la protección de datos personales y que identifiquen cuál es su contribución para el logro de los objetivos del SGSDP. Por ello, se deben establecer y mantener programas de capacitación que mantengan vigente al SGSDP como:

- a) **Concienciación:** programas a corto plazo para la difusión en general de la protección de datos personales en la institución.
- b) **Entrenamiento:** programas a mediano plazo que tienen por objetivo capacitar al personal de manera específica respecto a sus funciones y responsabilidad en el tratamiento y seguridad de los datos personales y;
- c) **Educación:** programa general a largo plazo que tiene por objetivo incluir la seguridad en el tratamiento de los datos personales dentro de la cultura de la institución.



Se debe realizar una detección de necesidades para identificar el nivel y tipo de capacitación necesaria para el personal, de acuerdo con las responsabilidades asignadas y tomando en cuenta su perfil de puesto, especialmente de aquéllos involucrados en el tratamiento de datos personales.

Estos programas de capacitación deben tomar en cuenta elementos como:

a) Requerimientos y actualizaciones al contexto del SGSDP, considerando principalmente;

1. Administración y comunicación de actualizaciones y noticias de privacidad;
2. Manejo de solicitudes ARCO y recepción de quejas de los titulares de los datos;
3. Recolección y manipulación de datos personales;
4. Gestión de incidentes y vulneraciones de seguridad;

b) La legislación en protección de datos personales y mejores prácticas relacionadas al tratamiento de datos aplicables a nuestra institución.

c) Las consecuencias del incumplimiento a los requerimientos mandados por la legislación general y local en la materia;

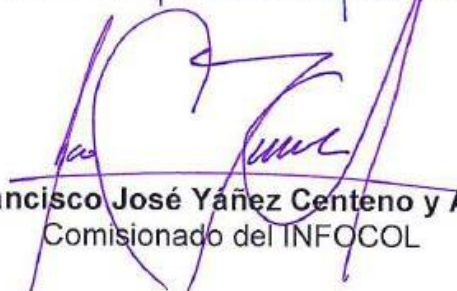
d) Las herramientas normativas y tecnológicas relacionadas o utilizadas para el tratamiento de datos personales y para la implementación de medidas de seguridad.

Finalmente se debe evaluar la eficiencia y eficacia de la capacitación, esta evaluación se puede llevar a cabo mediante la aplicación de exámenes teóricos o prácticos que permitan indicar el grado de conocimiento y/o entendimiento de la capacitación proporcionada o difusión realizada. Se deben establecer criterios de evaluación que determinen el nivel de competencia aceptado por nuestra institución, y mantener un registro de los programas seguidos por cada empleado, así como de sus habilidades, experiencia y calificaciones.

**FIRMAN EL PRESENTE DOCUMENTO LOS COMISIONADOS Y LA SECRETARIA EJECUTIVA DEL INFOCOL.**



**Mtro. Christian Velasco Milanés**  
Comisionado Presidente del INFOCOL



**Lic. Francisco José Yáñez Centeno y Arvizu**  
Comisionado del INFOCOL



**Lic. Carmen Iliana Ramos Olay**  
Secretaria Ejecutiva

*- - - La presente hoja de firmas forma parte de este documento del Sistema de Gestión de Seguridad de los Datos Personales del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima (INFOCOL), que consta de 66 fojas útiles, aprobado en la Sesión extraordinaria del pleno de este instituto, celebrada en fecha 17 diecisiete de diciembre del 2021 dos mil veintiuno.*



## **SISTEMA DE GESTIÓN DE SEGURIDAD DE LOS DATOS PERSONALES DEL INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS DEL ESTADO DE COLIMA**