INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE CHIAPAS

ESCUELA DE TRANSPARENCIA Y FORMACIÓN CIUDADANA

ESCUELA DE TRANSPARENCIA
Y FORMACIÓN CIUDADANA

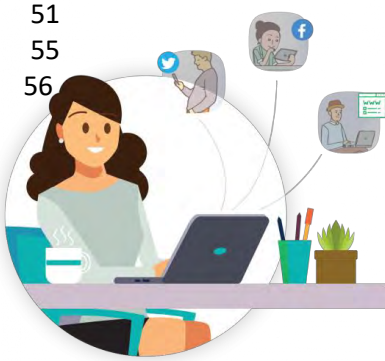
ITAIP CHIAPAS

Guía para la redacción del Documento de Seguridad

Ley de Protección de Datos Personales en Posesión de Sujetos obligados de Chiapas

Guía para la redacción del Documento de Seguridad

Contenido



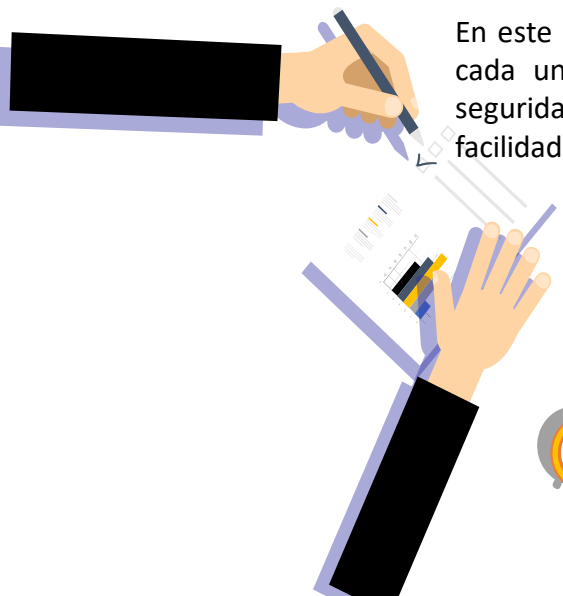
PRESENTACIÓN

La Guía para la Redacción del Documento de Seguridad ha sido diseñada pensando en facilitar este ejercicio, con el cual, los sujetos obligados estarán garantizando que se cumple la Ley de protección de Datos Personales del Estado de Chiapas (LPDPPSOCH).

Lo anterior es importante porque es nuestra responsabilidad como servidores públicos, garantizar a la ciudadanía, que al entregarnos sus datos para realizar un trámite o gestión o solicitar un servicio, no estará poniéndose en riesgo de que su identidad y privacidad sean vulneradas.

La LPDPPSOCH establece como una de las obligaciones, la redacción del documento de seguridad, en el que se de cuenta de las medidas de seguridad implementadas y las acciones que desarrollamos en las instituciones para garantizar la integridad de la información que recibimos.

La idea es que con el apoyo de la guía, los sujetos obligados comprendan el contenido de cada aspecto, apliquen los instrumentos y desarrollen el inventario de datos personales y tratamientos, el análisis de brecha y de riesgo y redacten el informe correspondiente, en el que incluyan una propuesta de capacitación para el personal.



En este sentido, la Guía ofrece un seguimiento paso a paso de cada uno de los elementos que integran el documento de seguridad, de tal forma que el lector podrá desarrollaros con facilidad y eficiencia, de manera autodidacta y con precisión.

Además de lo anterior, podrán apoyarse en los videos alojados en la página web del Instituto de Transparencia, Acceso a la información y Protección de Datos Personales de Chiapas (ITAIPCH), en la siguiente liga:

http://transparenciachiapas.org/capacitacion/

OBJETIVO

Promover la generación de conocimiento útil para el diseño del Sistema de gestión de Protección de Datos Personales y la redacción del Documento de Seguridad correspondiente a cada Sujeto Obligado, que garantice la observancia de los principios de protección de datos personales previstos en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas

ANTECEDENTES

La Ley De Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Chiapas busca garantizar el derecho de las personas a la protección de sus datos personales que estén en poder o posesión de todo ente público de los tres órdenes y niveles de gobierno, así como de los partidos políticos y otros sujetos obligados.

Para ello, establece que:

Artículo 48.- Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.

Artículo 49.- El responsable deberá elaborar y aprobar un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo conforme a lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia.

El documento de seguridad será de observancia obligatoria para los encargados y demás personas que realizan algún tipo de tratamiento de datos personales

1. ELEMENTOS CONCEPTUALES

a) ¿Qué son los datos personales?

Es toda información concerniente a una persona física que permitirá identificarla.

Se expresan de forma numérica, alfabética, alfa numérica, fotográfica, acústica o de cualquier otra manera.

Los datos personales puede ser:

De identificación: Nombre, edad, domicilio particular, sexo, RFC, CURP, etc.

Patrimoniales: Número de cuenta bancaria, saldos, propiedades, etc.

Sensibles: Refieren la esfera más íntima de su titular; revelan aspectos como origen racial o étnico, estado de salud pasado, presente o futuro, creencias religiosas, filosóficas y morales, opiniones políticas, datos genéticos, datos biométricos y preferencia sexual.

Su utilización indebida puede dar origen a discriminación o representar un riesgo grave para la persona; lo que implica un mayor compromiso con su protección y uso.

b) Marco Legal

Artículo 16º Constitucional

"Toda persona tiene derecho a la protección de sus datos personales, al **acceso, rectificación y cancelación** de los mismos, así como a manifestar su **oposición**, en los términos que fije la ley.…"

•Acceso

El titular tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, así como a conocer la información relacionada con las condiciones, generalidades y particularidades de su tratamiento. Artículo 60.

•Rectificación

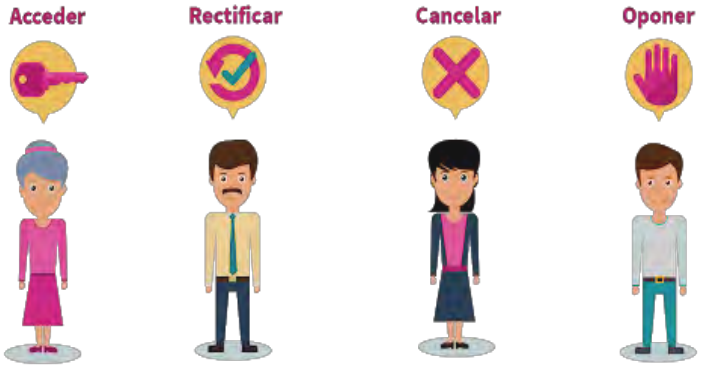
El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados. Artículo 61

•Cancelación

El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión. Artículo 62

•Oposición

El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando exista una causa legítima y su situación específica así lo requiera o sus datos sean objeto de un sistema automatizado con efectos jurídicos



Derechos ARCO

c) El deber de seguridad

El Artículo 45 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados de Chiapas, establece que el deber de seguridad implica la implementación de Medidas de seguridad de carácter administrativo, físico y técnico cuya finalidad es protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad

Las medidas de seguridad son el conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.

1. Medidas de seguridad físicas

Son Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento

a) Prevenir que el acceso no autorizado;

b) Prevenir el daño a las instalaciones;

c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico

d) proveer a los equipos un mantenimiento eficaz que asegure su disponibilidad e integridad;

2. Medidas de seguridad técnicas

Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento.

a. Prevenir que el acceso a las bases de datos o a la información;

b. Generar un esquema de privilegios;

c. Revisar la configuración de seguridad

d. Gestionar las comunicaciones, operaciones y medios de almacenamiento;

e. Medidas de seguridad administrativas

f. Políticas y Procedimientos

g. La identificación y clasificación de la información

h. Sensibilización y capacitación del personal

i. Documentos necesarios para la seguridad de la información

3. Medidas de seguridad administrativas

Son el conjunto de Políticas y Procedimientos para garantizar la protección de datos personales mediante la implementación de acciones relacionadas con:

a. La identificación y clasificación de la información

b. Sensibilización y capacitación del persona

c. Documentos necesarios para la seguridad de la información

d) Sistema de Gestión

Se entenderá por sistema de gestión al conjunto de acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión, integrado por un conjunto de elementos y actividades interrelacionadas para

- Establecer
- Implementar
- Operar
- Monitorear
- Revisar
- Mantener y
- Mejorar el tratamiento y seguridad de los datos personales

Documenta y contiene las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales

(LPDPPSOCH Artículo 48.)

Elementos de base para el Sistema de Gestión

2. DESARROLLO DE LA POLÍTICA DE GESTIÓN

Como parte del desarrollo de la política de gestión de datos personales, se identificarán las obligaciones que se deberán cumplir en los tratamientos, según el ciclo de vida de los datos personales, desde su obtención, durante el uso y hasta su eliminación una vez que ha sido concluido el tratamiento para el que fueron otorgados.

a) Documento de Seguridad

Para garantizar el desarrollo del Sistema de Gestión, la LPDPPSOCHIS establece:

Artículo 49.- El responsable deberá elaborar y aprobar un documento que contenga las medidas de seguridad de carácter físico, técnico y administrativo conforme a lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia.

Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

El documento de seguridad **será de observancia obligatoria** para los encargados y demás personas que realizan algún tipo de tratamiento de datos personales.

b) La Construcción del Documento de Seguridad

Para el logro de la protección de datos personales, lo primero que tenemos que hacer es un programa en el que se incluyan todos los elementos involucrados, es decir, tenemos que realizar un inventario de datos personales y de tratamientos, el análisis de riesgo y brecha, el procesos de revisión y monitoreo de las medidas de seguridad, el procedimiento para eliminar y suprimir los datos cuando ya no se usen, y planear la capacitación correspondiente.

Cada uno de estos elementos representan una serie de acciones a desarrollar para recuperar la información concerniente a la forma como se protegen los datos personales y la meta a alcanzar en dicho procesos.

El principio de esta guía es ofrecer herramientas para su logro.

Documento de Seguridad

- Identificación de tratamientos y datos personales
- El inventario de datos personales y de los sistemas de tratamiento
- Análisis de riesgo y de brecha
- Desarrollo de procedimientos y mecanismos para la conservación y supresión de datos personales;
- Programa de revisión y monitoreo de la efectividad del programa
- Programa de capacitación y actualización

c) Identificación de Datos Personales y Tratamientos

El primer paso es identificar los tratamientos, que son las operaciones llevadas a cabo durante el ciclo de vida de los datos personales, desde el momento de su obtención, pasando por su explotación o aprovechamiento, hasta su supresión o eliminación.

Al mismo tiempo es necesario identificar los datos personales utilizados en cada tratamiento.

El formato incluye

- Sujeto obligado o institución
- Unidad Administrativa
- Departamento
- Tratamiento o proceso
- Funcionarios que tratan datos personales (nombre y función)
- Datos personales que utiliza, considerando tipo de datos (identificativos, patrimoniales, sensibles)

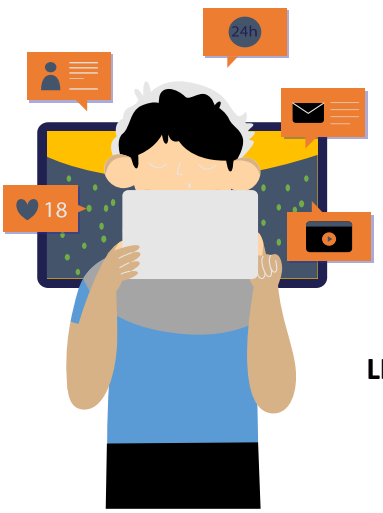
LLENAR ANEXO 1. CATALOGO DE DATOS PERSONALES

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, estructuración, adaptación, modificación, extracción, consulta, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, transferencia y en general cualquier uso o disposición de datos personales. (Artículo 5, Frac. XXXV LPDPPSOCH)

d) Inventario de Datos Personales y Tratamientos

El Artículo 47 en su fracción III, establece la necesidad de elaborar un inventario de los datos personales y/o sistemas de tratamiento; que consiste en un documento en el que daremos cuenta de:

1. Tratamientos de datos personales que se realizan
2. Unidad administrativa a cargo de estos procesos
3. Será necesario determinar, de acuerdo con el ciclo de vida de los datos personales:
   a. ¿Cómo se obtienen los datos personales?
   b. ¿Qué tipo de datos personales se tratan? ¿son sensibles?
   c. ¿Dónde se almacenan y realiza el tratamiento de los datos personales?
   d. ¿Para qué finalidades se utilizan los datos personales?
   e. ¿Quién tiene acceso a la base de datos o archivos (sistemas de tratamiento) y a quién se comunican los datos personales al interior del sujeto obligado?
   f. ¿Intervienen encargados en el tratamiento de los datos personales? ¿Cuál es el instrumento mediante el cual se formaliza su intervención?
   g. ¿Qué transferencias se realizan o se podrían realizar de los datos personales y con qué finalidad?
   h. ¿Se difunden los datos personales?
   i. ¿Cuál es el plazo de conservación de los datos personales?



LLENAR ANEXO 2. Inventario de datos personales y tratamientos

e) Análisis de Riesgo de los Datos Personales

La fracción IV del artículo 5 señala que hay que realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, hardware,
software, personal del responsable, entre otros.

Para ello hay que considerar:

I. Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
II. El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;
III. El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
IV. Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida;
V. El riesgo inherente a los datos personales tratados, contemplando el ciclo de vida de los datos personales, las amenazas y vulnerabilidades existentes para los datos personales y los recursos o activos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal o cualquier otro recurso humano o material, entre otros;
VI. La sensibilidad de los datos personales tratados;
VII. El desarrollo tecnológico;
VIII. Las transferencias de datos personales que se realicen;
IX. El número de titulares;
X. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
XI. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

Las medidas de seguridad que deberán adoptarse por el responsable deben tomar como referencia el nivel de riesgo que presenta cada tratamiento de datos personales.

Para ello, es necesario calcular los factores de riesgo **por tipo de dato, por número de usuarios por tipo de acceso, y por entorno** desde el cual se realizan los tratamientos de los datos personales

Tipos de Riesgo

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos	Bajo	1
Datos laborales, patrimoniales, procedimientos administrativos	Medio	2
Datos de tránsito y movimientos migratorios; de salud, biométricos	Alto	3
Datos sensibles	Muy alto	4-5

El nivel de riesgo por tipo de dato en relación con el número de titulares, servirá para determinar los controles que se deben considerar para su protección.

Es necesario tomar en cuenta también el volumen de titulares con los que trabajamos, teniendo en cuenta que a mayor número de titulares, mayor será el riesgo por tipo de dato. Es decir, el riesgo inherente más el volumen de titulares, da como resultado el nivel de riesgo por tipo de dato:

TIPO DE DATO	NÚMERO DE TITULARES			
	>100	>1000	>10,000	<10,000
Datos especialmente sensibles	**4**	**4**	**5**	**5**
Datos de tránsito y movimientos migratorios; de salud, biométricos	**1**	**2**	**3**	**3**
Datos laborales; patrimoniales; procedimientos administrativos	**1**	**1**	**2**	**2**
Datos identificativos.	**1**	**1**	**1**	**1**

Además, el riesgo por tipo de acceso se mide determinando la cantidad de accesos potenciales a los datos personales que se pretenden proteger en un intervalo de tiempo, por ejemplo, durante 24 horas. Para este parámetro entre mayor sea la accesibilidad, mayor riesgo existe para la información.

Es necesario determinar la cantidad de accesos a la información: 10, 20, 30, 40 veces y la valoración en cada caso, de acuerdo con la tabla siguiente:

TIPO DE ACCESOS	RIESGO INHERENTE	NIVEL DE RIESGO
10 veces	Bajo	1
20 veces	Medio	2
30 veces	Alto	3
40 veces	Muy alto	4-5

Finalmente, en el riesgo por tipo de entorno este factor representa el nivel de anonimidad para acceder o hacer uso de los datos personales que se tratan.

Entre mayor anonimidad ofrezca el entorno, mayor riesgo existe de que se vulnere la seguridad.

En caso de que se accedan por más de un entorno a los datos personales, se debe considerar el entorno de mayor riesgo.

ENTORNO	NIVEL DE RIESGO
Físico	1
Equipo de cómputo	2
Nube	3
Internet	4

Cada área identificará el nivel de riesgo en que se encuentran los datos personales a partir de:

El tipo de dato,
el volumen,
el número de accesos y
el entorno en el que se almacena

Se realiza el análisis por tratamiento seleccionando el número correspondiente de acuerdo con el manejo que se hace de los datos personales en todos los tratamientos, se suman todos los valores seleccionados y se dividen entre 4 para obtener el riesgo inherente de cada tratamiento.

Nombre del tratamiento _____				
FACTOR DE RIESGO	RIESGO INHERENTE			
Tipo de dato	Identificativos 1	Datos laborales, patrimoniales, procedimientos administrativos 2	Datos de tránsito y movimientos migratorios; de salud, biométricos 3	Datos sensibles 4-5
Volumen	Menos de 100 1	Menos de 1000 2	Menos de 10000 3	Mas de 10000 4-5
Accesos	10 1	20 2	30 3	40 4
Entorno	Físico 1	Equipo de cómputo 2	Nube 3	Internet 4
total de riesgo inherente	(suma de todos los valores seleccionados y divididos entre 4)			

Posteriormente, se integrarán todos los análisis por tratamiento, para realizar un cuadro en el que se señale por unidad administrativa, área o dirección, las medidas de seguridad implementadas, las medidas de seguridad faltantes y el riesgo inherente en que se encuentran los datos personales.
Se sumarán todos los valores de riesgo inherente y se dividirán entre el número de tratamientos que realiza el área o dirección en cuestión, el resultado será el riesgo inherente de cada dirección.

Dirección o área _____					
Análisis de riesgo					
Tratamiento	Tipo de dato	Volumen	Accesos	Entorno	Promedio de riesgo inherente
Promedio total					00.00

La combinación de los cuatro factores analizados da como resultado el nivel de riesgo latente de cada tratamiento de datos personales, lo cual contribuye a identificar el nivel de medidas de seguridad que deben implementarse en cada caso.

Una vez que se calcula el nivel de riesgo latente por cada tratamiento de datos personales, es posible realizar estrategias para identificar los modelos de medidas de seguridad que deben aplicarse a cada uno de ellos.

Realizar un análisis de riesgos por cada tratamiento ayudará a identificar las medidas de seguridad que deben ser implementadas para la protección de los datos personales.

Posteriormente, se realiza un comparativo con aquellas que son implementadas por las áreas, obteniendo con ello un análisis de brecha, a través del cual se construirán los planes de trabajo, mecanismos de monitoreo y revisión de medidas de seguridad y programas de capacitación necesarios

Para realizar el análisis de riesgo, utilizar el anexo 3.

f) Análisis de Brecha

La fracción V del Artículo 5, establece que es necesario realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.

El análisis de brecha consiste en identificar la distancia que existe entre las medidas recomendadas y las medidas implementadas por cada uno de los tratamientos reportados.

Este análisis es de naturaleza diagnóstica y contribuye a conocer las áreas de oportunidad por cada tratamiento. Implica que se logre realizar un comparativo entre las medidas implementadas por las áreas y las que tendría que implementar; con esta información podrá desarrollarse:

- Los planes de trabajo,
- Mecanismos de monitoreo y revisión de medidas de seguridad y
- Programas de capacitación necesarios

Por ejemplo, si se recomienda implementar al tratamiento "A" un conjunto de medidas "C", y el área responsable de dicho tratamiento informa que de ese conjunto de medidas hacen falta implementar algunas, la identificación de lo que hace falta implementar se conoce como brecha.

Para su realización, se tomará en cuenta lo siguiente:

Las medidas de seguridad existentes y efectivas;
Las medidas de seguridad faltantes, y
La existencia de nuevas medidas de seguridad que pudieran remplazar a uno o más controles implementados actualmente.

LLENAR EL ANEXO 3. Análisis de brecha

3. REDACCIÓN DEL DOCUMENTO DE SEGURIDAD

Una vez que hemos identificado los datos y tratamientos con los que trabajamos y se han realizado el inventario de datos personales, el análisis de riesgo y el análisis de brecha, se procederá a redactar el documento de seguridad, en el que se presentará de manera gráfica, el análisis de los resultados de los ejercicios antes mencionados, con las explicaciones necesarias que permitan comprender el proceso de protección de datos personales que se desarrolla en la institución.

La redacción del documento de seguridad es una actividad que debe desarrollarse de forma interdisciplinaria (con representantes de cada área destinados a dar seguimiento al programa).

A continuación se presentan ejemplos de redacción de cada uno de los apartados que integran el Documento de Seguridad, con el propósito de ayudar a generar ideas para la redacción del propio en cada institución.

a) Contenido del Documento de Seguridad

Presentación
Objetivos del documento de seguridad
Responsabilidades
Alcance del documento de seguridad
Sistema de Gestión de los datos personales
Inventario de tratamientos y datos personales
Funciones y responsabilidades del tratamiento de datos personales
Programa de trabajo para la implementación de medidas de seguridad
Análisis de riesgo y brecha
Análisis de la información
Medidas de seguridad
Monitoreo de medidas de seguridad
Propuesta de capacitación en materia de datos personales

b) Objetivos del Documento de Seguridad

Ejemplo de redacción

El presente programa tiene como objetivos los siguientes:

1. Proveer el marco de trabajo necesario para la protección de los datos personales en posesión de (el sujeto obligado);

2. Cumplir con las obligaciones que establece, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del estado de Chiapas y los Lineamientos Generales, así como la normatividad que derive de los mismos;

3. Establecer los elementos y actividades de dirección, operación y control de los procesos que impliquen el tratamiento de datos personales, a efecto de protegerlos de manera sistemática y continua, y

4. Promover la adopción de mejores prácticas en la protección de datos personales, de manera preferente una vez que el programa se haya implementado de manera integral en la organización, o bien, cuando se estime pertinente la implementación de buenas prácticas en tratamientos específicos.

c) Responsabilidades Dentro del Programa

Ejemplo de redacción

Con fundamento en lo dispuesto por los artículos 113 y 114, de la LPDPPSO de Chiapas, que señalan que el Comité de Transparencia es la autoridad máxima en materia de protección de datos personales y que tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, dicho órgano tendrá las siguientes funciones en relación con este programa:

I. Aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia.
II. Coordinar, realizar y supervisar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en las que resulten aplicables en la materia, en coordinación con el oficial de protección de datos personales, en su caso.
III. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.
IV. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se declare improcedente, por cualquier causa, el ejercicio de alguno de los derechos ARCO.

V. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se declare improcedente, por cualquier causa, el ejercicio de alguno de los derechos ARCO.

VI. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad
VII. Coordinar el seguimiento y cumplimiento de las resoluciones emitidas por el Instituto.
VIII. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales.

(ejemplo de redacción)

Anualmente se presentará un informe, en las primeras dos semanas del mes de marzo de cada año y referirá al año inmediato anterior. Algunos de los elementos que pueden incluirse en el informe son:

- Estadística e información general sobre el cumplimiento de las obligaciones señaladas en el Programa de Protección de Datos Personales por parte de las unidades administrativas;

- Acciones realizadas por el Comité de Transparencia y la Unidad de Transparencia para cumplir con las obligaciones específicas que establece el Programa de Protección de Datos Personales, y

- Los resultados de las revisiones y auditorias.

La intervención de [nombre del puesto que encabeza al sujeto obligado] tendrá la finalidad única de impulsar la debida implementación del Programa al interior del sujeto obligado, pero no podrá suplir ni afectar las funciones que otorgan los artículos 113 y 114 de la LPDPPSO de Chiapas al Comité de Transparencia, en su carácter de máxima autoridad de datos personales en la institución.

Asimismo, para que la implementación del programa tenga como resultado el cumplimiento integral de las obligaciones que establece la LPDPPSOChis y los Lineamientos correspondientes, el programa será de observancia obligatoria para todos los servidores públicos del sujeto obligado que en el ejercicio de sus funciones traten datos personales.

Para que los objetivos planteados en la primera sección se logren con éxito, el Programa requiere del apoyo e impulso directo del más alto nivel de la institución. En ese sentido, el Programa se deberá hacer del conocimiento de [incluir nombre del puesto que encabeza el sujeto obligado, por ejemplo, del Secretario de Economía], a fin de que tome las medidas necesarias para que el mismo se observe en [nombre del sujeto obligado].

d) Alcance del Programa

(Ejemplo de redacción)

El presente programa aplicará a todas las unidades administrativas que realicen tratamiento de datos personales en ejercicio de sus atribuciones, y a todos los tratamientos de datos personales que éstas efectúen en ejercicio de sus atribuciones.

Se cubrirán todos los principios, deberes y obligaciones de la LPDPPSOCHIS:

… (Enumerar Art. 12, 13, 14 de la LPDPPSO Chiapas)

Las Unidades Administrativas involucradas son:

…

... (Listado de las unidades administrativas que manejan datos personales)

e) Redacción del Sistema de Gestión de los Datos Personales

Ejemplo de redacción

El tratamiento de datos personales que realicen las unidades administrativas deberá cumplir con los principios, deberes y obligaciones que prevé la LPDPPSOCHIS, para lo cual este programa establecerá el marco de trabajo mínimo que se deberá seguir para alcanzar dicho objetivo.

Para ello, se identificarán las obligaciones que se deberán cumplir en todos los tratamientos de datos personales que realicen las unidades administrativas, de acuerdo con lo que establece la LGPDPPSO y los Lineamientos Generales, y según el ciclo de vida de los datos personales

Asimismo, el sujeto obligado procurará la adopción de mejores prácticas para la protección de datos personales, en aquellos tratamientos que así lo permitan y según el nivel de madurez que exista.

Sistema de Gestión de los Datos Personales (continuación)

Se sugiere presentar un esquema como este o mediante la ilustración de su elección, presentando los tres momentos del ciclo de vida de los datos personales

Ejemplo de redacción:

En cumplimiento de deber de confidencialidad, la (institución) ha implementado mecanismos que garantizan la confidencialidad en las diferentes fases del tratamiento de los datos personales. Entre estas podemos contar con:

- La integración de cláusulas en los contratos de los encargados (cuando sea el caso) y el personal, que comprometen a la confidencialidad de los datos personales

- Se ha diseñado y aplicado una propuesta de capacitación dirigida al personal de (institución), encaminada a lograr la sensibilización y generar conciencia en torno a la necesidad de guardar confidencialidad. El programa se encuentra en el rubro de capacitación de este documento. (si la capacitación se ha llevado a cabo, incluir evidencia, por ejemplo el calendario)

La Unidad Administrativa (especificar área) realiza tratamiento de los datos personales en apego a sus atribuciones, fundadas en (artículo(s) de Ley, Lineamiento, Reglamento interno, que le faculta), que establece que (describir todas funciones o atribuciones para realizar los tratamientos). (redactar por cada unidad administrativa que recaba datos personales y porcada tratamiento).

Estas atribuciones están señaladas en los avisos de privacidad correspondientes a cada tratamiento, mismos que se encuentran a la vista del público y en el portal web de (Institución).

Nota: Esta redacción se hará por cada unidad administrativa y tratamiento

f) Inventario de Tratamientos de Datos Personales

Redacción con base en los inventarios que tienen por áreas:

Para el debido cumplimiento de las obligaciones que se establecen en este documento, fue necesario que cada una de las unidades administrativas realizaran un diagnóstico de los tratamientos de datos personales que llevan a cabo.

El diagnóstico en mención se basa en la elaboración de un inventario con la información básica de cada tratamiento de datos personales que se realizan en [*nombre de la institución*].

Por "inventario de tratamientos de datos personales" se entenderá el control documentado que se llevará de los tratamientos que realizan las unidades administrativas de [*nombre de la institución*], realizado con orden y precisión.

A continuación se presenta la información respecto a los tratamientos que realiza cada Unidad Administrativa.

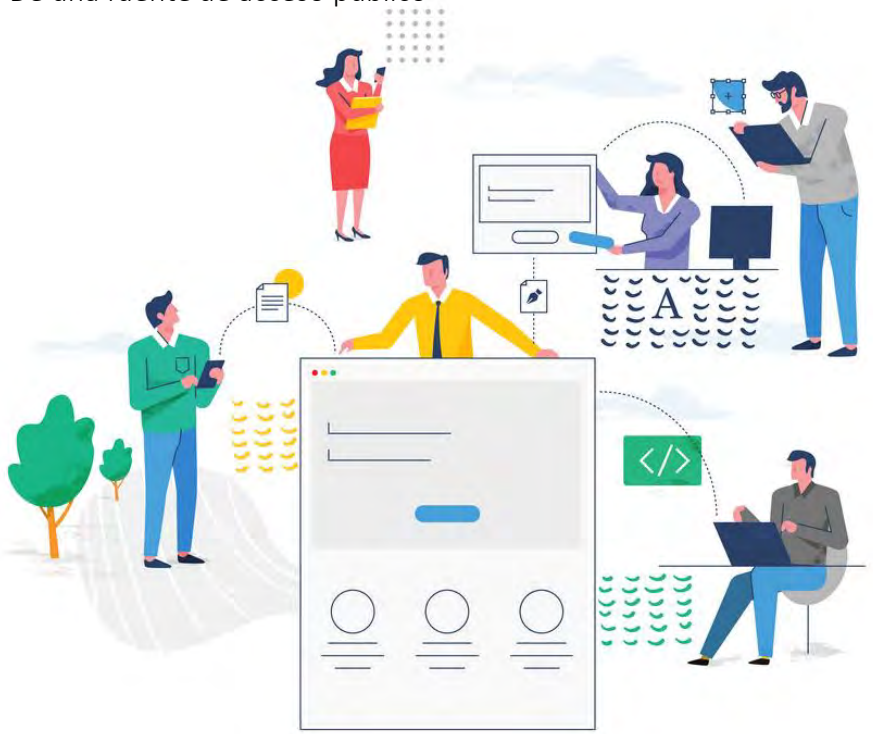
UNIDAD ADMINISTRATIVA	ÁREA	TRATAMIENTO(S) O PROCESO (S)
(Nombre de la dirección a donde está adscrito el departamento o área) Por ejemplo: Dirección de administración y Finanzas	(Departamento responsable del proceso o tratamiento) Por ejemplo: Recursos Humanos	Contrataciones
		Integración de expediente de personal
		Pago de nómina
		Inscripción al IMSS
	Recursos materiales	Tratamiento 1…
		Tratamiento 2…
		Tratamiento 3…

Al cuadro se integrarán todas las áreas con sus respectivos departamentos y tratamientos

Ejemplo de redacción

Por otra parte, en lo que se refiere a los medios para la obtención de los datos, es preciso señalar que esto se lleva a cabo por los siguientes:
(se seleccionarán los medios para la obtención de los datos, pueden hacerlo como listado o en un solo párrafo)

- Directamente del titular
- De manera personal, con la presencia física del titular de los datos personales o su representante, en su caso.
- Vía telefónica
- Por correo electrónico
- Por Internet o sistema informático
- Por escrito presentado directamente en las oficinas del sujeto obligado
- Por escrito enviado por mensajería
- Mediante una transferencia. Quién transfiere los datos personales y para qué fines, medios por los que se realiza la transferencia
- De una fuente de acceso público



Ejemplo de Redacción:

Entre estos, se recaban XXXXX (cantidad) datos identificativos, XXXXXX datos patrimoniales y XXXXX datos sensibles. Para su uso, se requiere, en el caso de los datos de identificación, consentimiento XXXX; en el caso de los datos patrimoniales, el consentimiento es XXXXX; y para el uso delos datos sensibles, el consentimiento debe ser XXXXX (Tácito, expreso, expreso y por escrito) (mencionar por cada tipo de dato el tipo de consentimiento que se requiere,

Datos personales identificativos	Datos personales patrimoniales	Datos personales sensibles
Nombre, domicilio, CURP, fotografía, huella digital, edad, clave de elector, estado civil, RFC, correo electrónico personal, teléfono, sexo, información académica, fecha y lugar de nacimiento, cédula profesional, nacionalidad, número de seguridad social …	Cuentas bancarias, estos de cuenta, CLABE interbancaria, institución bancaria, facturas, Descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil …	Datos de salud, lengua indígena, origen étnico, discapacidad …

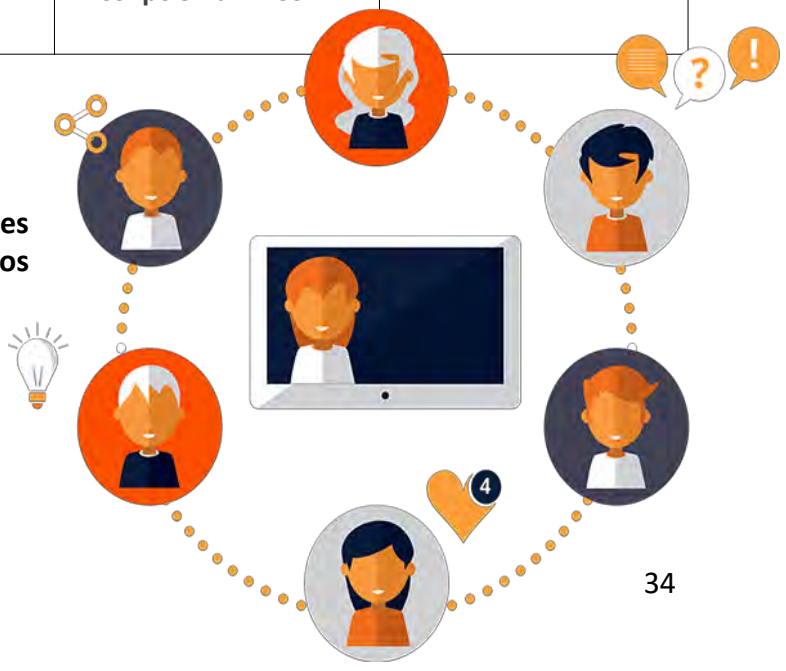
Al cuadro se integrarán todos los datos personales con los que se realizan todos los tratamientos de la institución.

Ejemplo de redacción:

Cada área realiza el tratamiento con una finalidad definida por sus funciones, tal como se señala en el cuadro siguiente:

Unidad administrativa o dirección	Departamento o área	Tratamiento	Finalidad
EJEMPLO: **Dirección de administración y finanzas**	**Recursos Humanos**	**Ejemplo:** el tratamiento podría ser **"contratación de personal"**	La finalidad puede ser "**evaluación de currículum para la selección de personal**".
		Integración de expediente de personal	
		Pago de nómina	
		Inscripción al IMSS	

Al cuadro se integrarán las finalidades de todas las áreas con sus respectivos departamentos y tratamientos



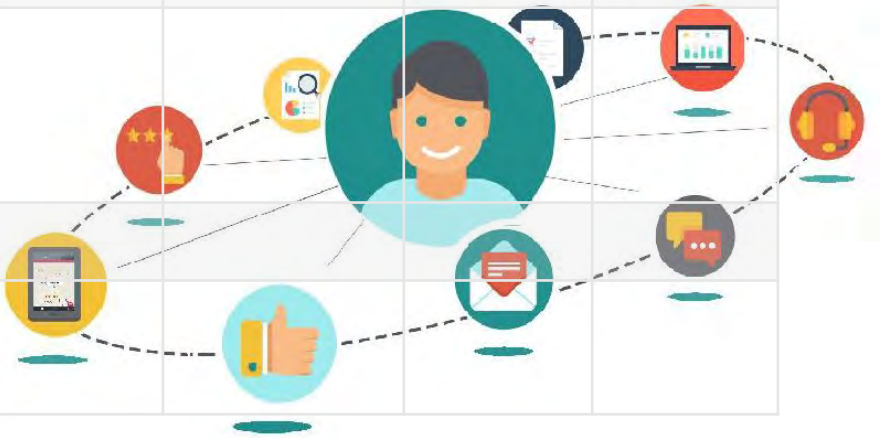
Ejemplo de Redacción:

Los funcionarios que, dadas sus atribuciones, tienen acceso a los datos son:

Unidad administrativa	Departamento o área	Tratamiento	Personas que tienen acceso a los datos
EJEMPLO: Dirección de administración y finanzas	Recursos Humanos	Contrataciones	**Nombres del (los) funcionario(s)**
		Integración de expediente de personal	
		Pago de nómina	
		Inscripción al IMSS	

Al cuadro se integrarán los nombres de los funcionarios que tienen acceso a los datos personales de todas las áreas con sus respectivos departamentos y tratamientos

Ejemplo de redacción:
Como parte del proceso, se transfieren datos personales a las siguientes instituciones y se difunden a otras áreas, con las finalidades señaladas en el cuadro siguiente:

Unidad administrativa o dirección	Tratamiento	Institución o empresa a la que se transfieren los datos personales	¿Se requiere consentimiento? Señalar si es Tácito, expreso, expreso y por escrito	¿Se difunden a otras áreas de la misma institución? Señalar a cuales	Finalidades de la transferencia o tratamiento
EJEMPLO: Dirección de administración y finanzas	Contrataciones	**Nombres de la(s) institución(es) o empresa(s)**			
	Integración de expediente de personal				
	Pago de nómina				
	Inscripción al IMSS				

Cuando se trata datos personales sensibles, el consentimiento debe ser expreso

Ejemplo de redacción:
El consentimiento expreso se solicita mediante **(puede ser una carta de consentimiento o una leyenda en el formulario para recabar datos, mismo que debe ser firmado por el titular. Especificar el procedimiento)**

Incluir en el reporte:

Cantidad de procesos y personas que utilizan datos personales:

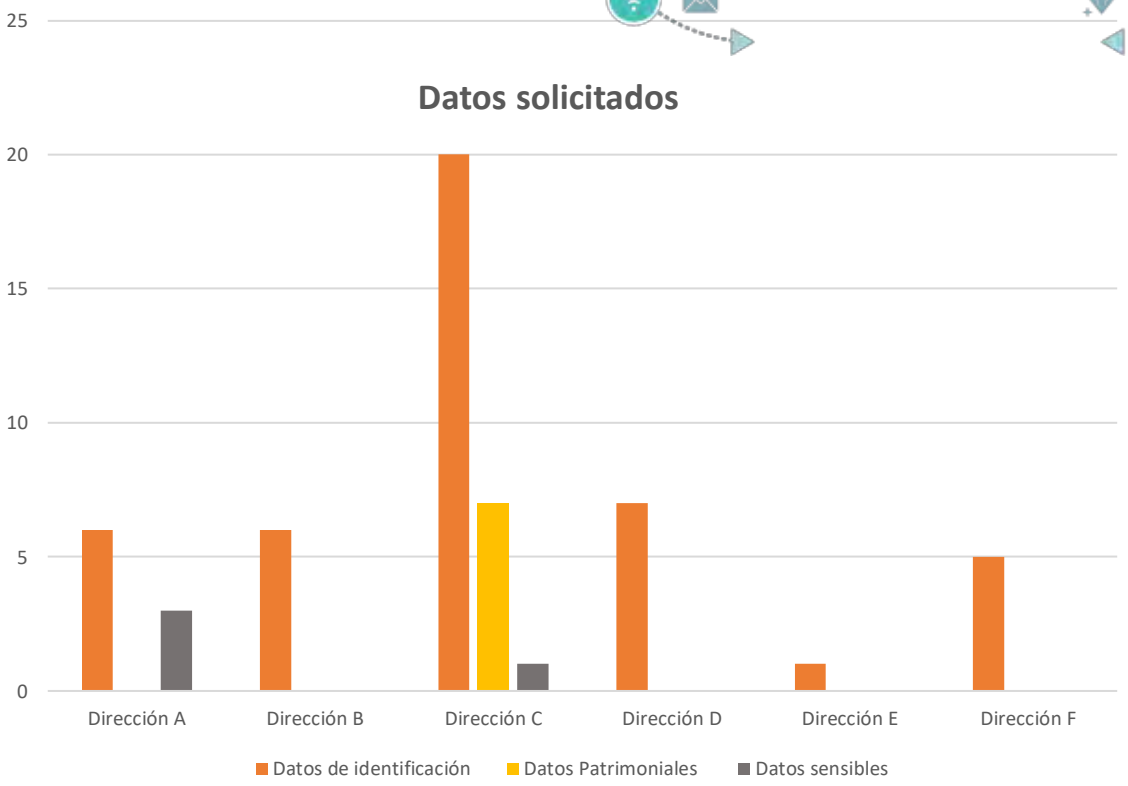
Ejemplo de redaccion:

Estos datos son utilizados en XXX procesos, de los cuales XXX corresponden a la dirección XXX, tres a la dirección de XXXX, siete a la dirección de XXXXXXXXX, uno a la dirección de XXXXX, tres a la dirección XXXXX y uno a XXX. Asimismo, en XXX procesos se utilizan datos personales de identificación, en XX se utilizan datos personales patrimoniales y en XXX procesos se utilizan datos sensibles.

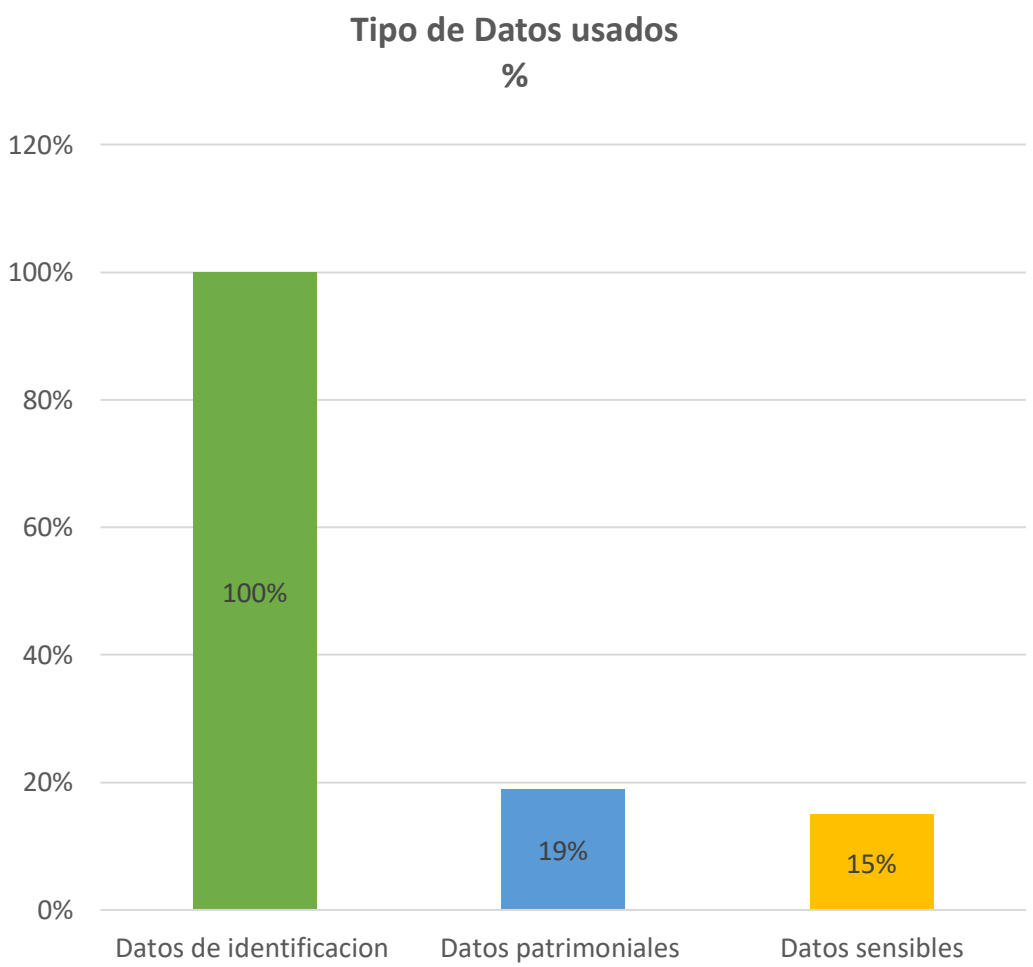
Como se puede apreciar, la unidad administrativa con mayor número de procesos es xxxx con xxx procesos, mientras que xxxx y la dirección de xxxx son las que menos procesos desarrollan, al ser solamente uno en cada área.

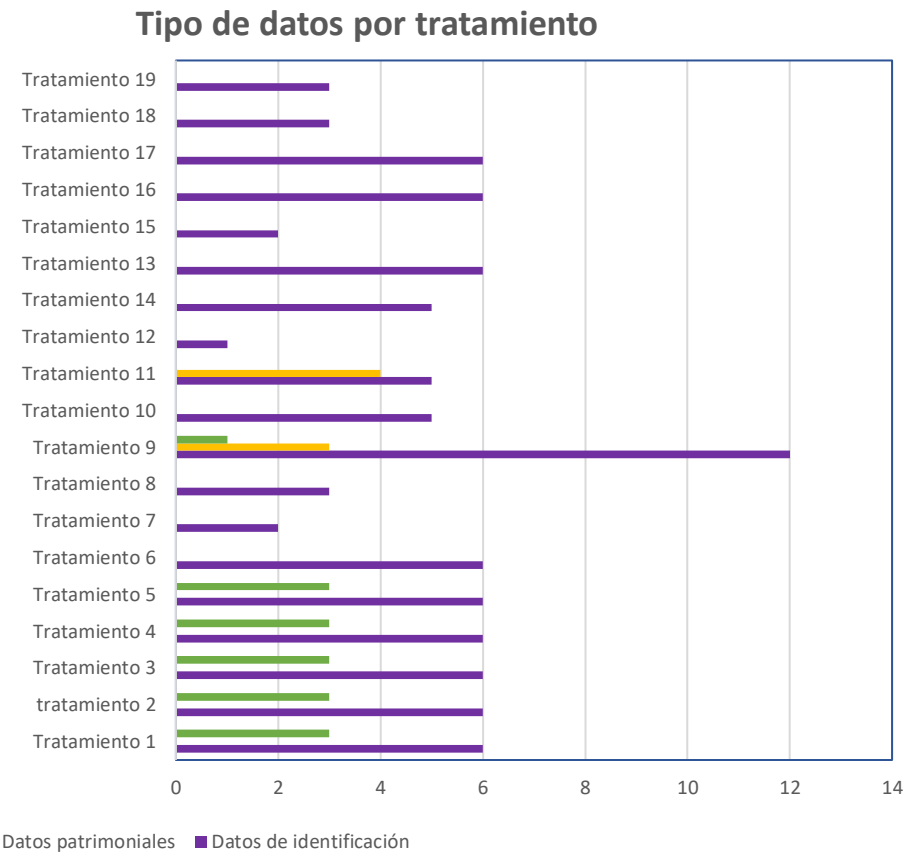
En relación con los datos solicitados, todas las unidades administrativas solicitan datos de identificación, mientras que solamente la dirección xxx solicita datos patrimoniales y algunos datos sensibles; tal como se presenta en la gráfica.

(Es recomendable incluir graficas que expresen porcentaje de tipo de dato, porcentaje de datos utilizados por unidades, gráfica de tipo de datos utilizados por cada unidad, unidad administrativa que desarrolla mayor número de procesos, de manera específica, como recaba los datos cada unidad)



A, B, C se sustituye con el nombre de la dirección correspondiente


Tipo de Datos usados
%
120%
100%
80%
60%
40%
20%
0%
100%
19%
15%
Datos de identificacion
Datos patrimoniales
Datos sensibles



Se deberá sustituir “1, …2, …3” por el nombre del tratamiento en cuestión

g) Redacción de Análisis de Riesgos y de Brecha

Ejemplo de redacción

El presente análisis identifica el riesgo inherente a los datos personales en el tratamiento que reciben por (nombre de la institución) al ejercer sus atribuciones, de manera que pueda ser controlado por la institución para satisfacer el derecho humano a la autodeterminación informativa.

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

Con base en la Ley, la valoración de los riesgos de los datos personales forma parte de los elementos mínimos que debe contener el instrumento que describe y da cuenta, en lo general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas (Documento de seguridad), en este caso, por (la institución), con el propósito de garantizar la confidencialidad, integridad y disponibilidad de ese tipo de datos bajo su posesión.

Aunado a lo anterior, el análisis de riesgos de los datos personales tratados debe contemplar los siguientes aspectos:

Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico.

El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida.

El valor y exposición de los activos involucrados en el tratamiento de los datos personales.

Las consecuencias negativas para los titulares de los datos personales, que puedan derivar en una vulneración de seguridad.

El riesgo inherente, la sensibilidad, las posibles consecuencias de vulneración para los titulares, las transferencias y vulneraciones previas ocurridas sobre los datos personales, así como el número de titulares de éstos y el riesgo por su valor potencial, además del desarrollo tecnológico.

h) Análisis de la Información

Se puede iniciar refiriendo el número de direcciones que tratan datos personales y el numero de tratamientos por unidad

Ejemplo de redacción:

Estado actual del riesgo de datos personales
En general se tiene que (la institución) cuenta con XXXX unidades administrativas en las que se da tratamiento de datos personales mediante xxx procesos como se visualiza a continuación:

UNIDAD ADMINISTRATIVA	TRATAMIENTOS
Escribir el nombre de cada unidad administrativa o dirección	El número de tratamientos que desarrolla

Ejemplo de redacción

Bajo esta premisa, para analizar los riegos de los datos personales que son objeto de tratamiento por (la institución), se aplicó un instrumento para, primeramente, clasificar los datos utilizados, a partir de la categorización existente en la ley:

1) De identificación o contacto, que se refieren a información por la que se identifica a una persona y/o permiten su contacto como, por ejemplo, el nombre, el domicilio, el correo electrónico, la firma, los usuarios, el Registro Federal de Contribuyentes, la Clave Única de Registro de Población o la edad.

2) Patrimoniales, que comprenden la información que se encuentran vinculados al patrimonio de una persona como, por ejemplo, el salario, los créditos, las tarjetas de débito, los cheques o las inversiones.

3) Sensibles, que consideran la información concerniente a la esfera más íntima de su titular o que su uso puede dar origen a discriminación o conlleva un riesgo grave para éste como, por ejemplo, el origen étnico, el estado de salud presente o futuro, las creencias religiosas, la opinión política o la orientación sexual.

De los anteriores, se identificó que se trabaja con (No. De categorías, 2 o 3): Datos de Identificación y datos patrimoniales, datos sensibles. Se recuperan datos de (incluir aquí los datos que se solicitan).

Ejemplo de redacción

Esto es, se tomó en cuenta la probabilidad baja, media o alta de que la amenaza suceda en las distintas etapas de vida de los datos personales.

Así, se consideró la consecuencia desfavorable leve, moderada o grave que al titular provoca en caso de que la amenaza ocurra (impacto).

La identificación y valoración del riesgo en cada proceso en que se tratan datos personales por las unidades administrativas de (la institución) se basaron en una escala del 0 al 3, representándose de la forma siguiente:

TIPO DE DATO	RIESGO INHERENTE	NIVEL DE RIESGO
Datos identificativos	Bajo	1
Datos electrónicos, de domicilio laborales, patrimoniales, procedimientos administrativos	Medio	2
Datos sensibles	Alto	3

NOTA: Para este análisis hay que considerar con qué tipo de datos trabajamos mayormente **y, a partir de eso, haremos un promedio. Por ejemplo, si trabajo sobre todo con datos sensibles el riesgo por tipo de dato será alto; pero si trabajamos sobre todo con datos identificativos y solamente algunos patrimoniales y sensibles, Podemos decir que el nivel de riesgo por tipo de dato será medio. Difícilmente será bajo, pues tendríamos que trabajar solamente con datos identificativos y eso no sucede.**

Ejemplo de redacción

Además, cuando hablamos de riesgo inherente, por el volumen de titulares contenidos en la base de datos, podemos decir que el riesgo es (Bajo, Medio o alto) ya que como vemos, hay XXXX unidades administrativas que manejan menos de 1000 titulares, mientras que XXXX unidades manejan mas de XXX:

Unidad administrativa	Volumen de datos	NIVEL DE RIESGO

Nota: Nuevamente se establece un promedio, a partir de las cantidades de datos que utiliza cada unidad administrativa: menos de 100 = 1, menos de1000 = 2, Menos de 10 000 = 3, más de 10 000 = 4

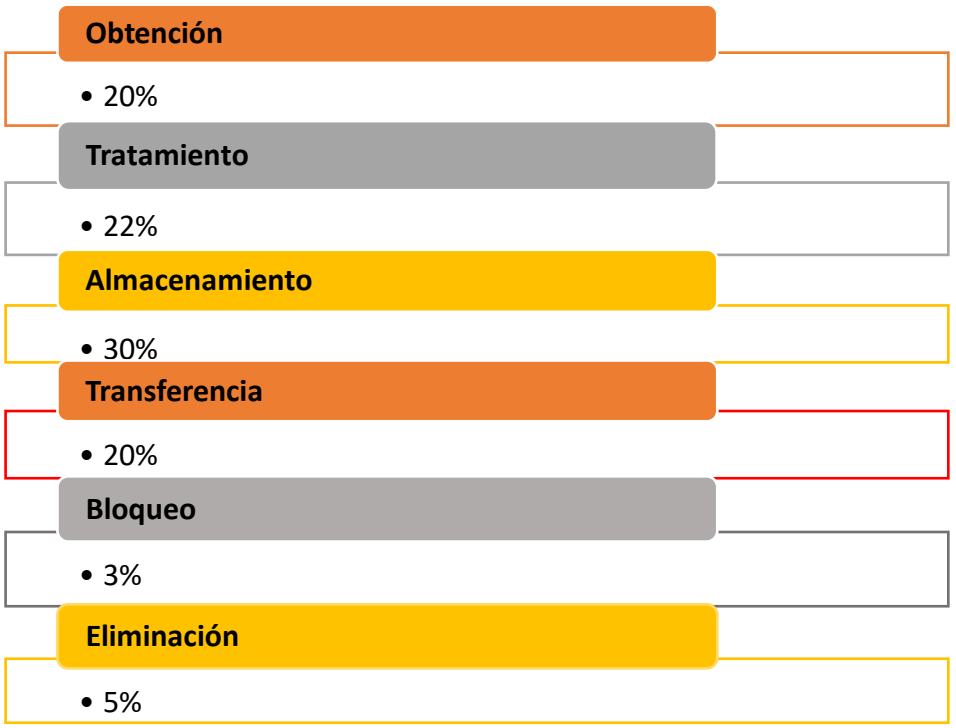
Ejemplo de redacción

La unidad administrativa que observa mayor estado de vulnerabilidad y riesgo inherente de los datos personales es la dirección XXXXX con 1.5 de riesgo, seguida en orden descendente por la dirección de XXX de con 1.25 de riesgo, las direcciones de XXX y de XXX con 1.0 de riesgo, y la dirección de XXX y la dirección de XXX con 0.75 de riesgo, tal como se muestra en la gráfica.

NOTA: La identificación de la etapa de mayor y menor vulnerabilidad es el resultado de la valoración que se haga al distribuir porcentajes a las etapas del tratamiento (obtención, tratamiento, almacenamiento, transferencia, bloqueo y eliminación), analizando cual es el riesgo para cada etapa, de acuerdo con las medidas de seguridad que implementamos y los diferentes entornos. **Es resultado del concentrado de la página 19**

Etapa de mayor y menor vulnerabilidad

Al respecto, hay que señalar además que la etapa del ciclo de vida (obtención, tratamiento, almacenamiento, transferencia, bloqueo y eliminación) en la que los datos personales se encuentran más vulnerables, es en el periodo de almacenamiento en un XX%; mientras que el periodo que implica menor riesgo es el de bloqueo con un XX%

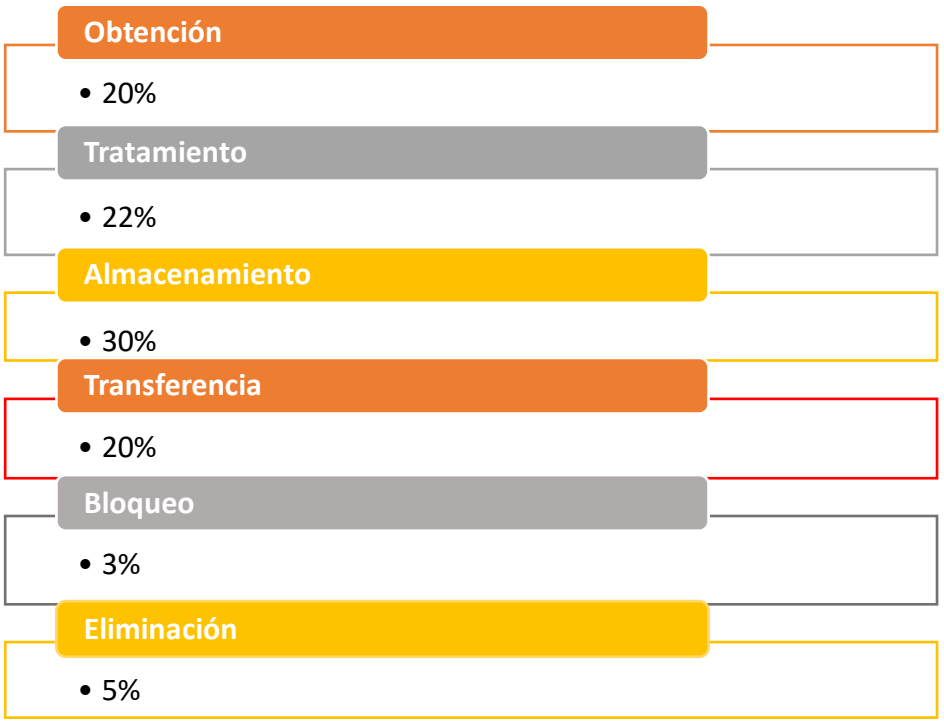


Nota: Esta valoración es resultado del análisis cualitativo que se realiza en equipo, a partir de las condiciones y realidad institucionales, distribuyendo el 100% entre el total de elementos considerados para el ciclo de vida de los datos personales

Ejemplo de redacción

En un segundo momento, para la determinación del riesgo sobre esa tipología de datos personales se valoró la probabilidad e impacto de que, en su obtención, almacenamiento, tratamiento, transferencia o remisión, bloqueo y/o eliminación (ciclo de vida), en correspondencia con la cantidad de datos involucrados, se materialice uno o más factores que pueden causar un daño a su titular (amenaza).

Al respecto, hay que señalar además que la etapa del ciclo de vida en la que los datos personales se encuentran más vulnerables, es en el periodo de almacenamiento en un 30%; mientras que el periodo que implica menor riesgo es el de bloqueo con un 3%.



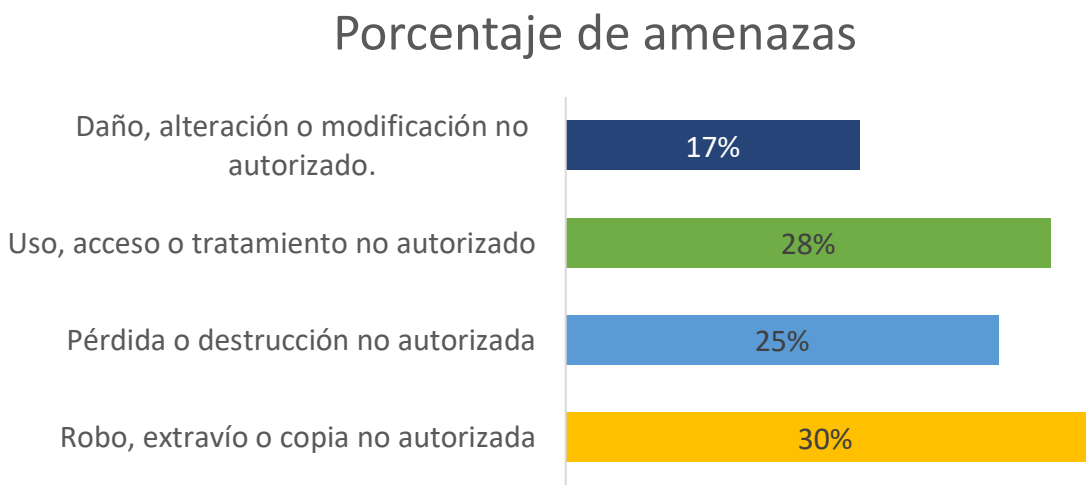
Nota: Esta valoración es resultado del análisis cualitativo que se realiza en equipo, a partir de las condiciones y realidad institucionales, distribuyendo el 100% entre el total de elementos considerados para el ciclo de vida de los datos personales

Ejemplo de redacción

Las amenazas a las que se ven expuestos son básicamente:

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

Siendo la más alta, la de robo, extravío o copia no autorizada y la de menor riesgo es daño, alteración o modificación no autorizada, como se muestra en la tabla siguiente:

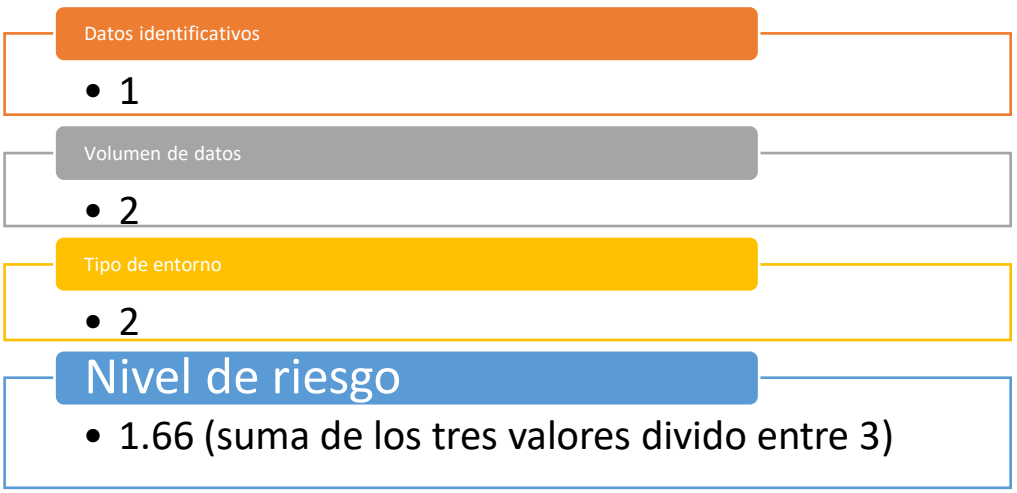


NOTA: Esto también corresponde a una valoración en equipo acerca de las amenazas a las que están expuestos, de acuerdo con los resultados de la brecha, es decir, las medidas de seguridad pendientes de implementar

Ejemplo de redacción

La unidad administrativa que observa mayor estado de vulnerabilidad y riesgo de los datos personales es (xxxxx) con XXX de riesgo, seguida en orden descendente por la dirección de (XXXX) de con XXX de riesgo, la dirección de XXX con XXXXX de riesgo.

Finalmente, como parte del análisis es posible establecer que el nivel de riesgo es mayormente (bajo, medio alto), debido que se trabaja sobre todo con datos de identificación, en algunos casos con datos patrimoniales y son en un tratamiento se solicita un dato sensible.
Asimismo, los datos personales corresponden a menos de 1000 personas, lo que reduce el nivel de riesgo y se mantienen a resguardo en computadoras personales con contraseña y en archiveros con llave para ampliar el margen de seguridad.



1 - 1.4 = bajo 1.5 - 2.4 = medio 2.5 – 4 = alto

(NOTA: ESTE ANÁLISIS ES RESULTADO DEL CRUCE QUE HICIERON DE RIESGO POR TIPO DE DATO, NÚMERO DE DATOS, NÚMERO DE ACCESOS Y ENTORNO DE ALMACENAJE)

i) Redacción de Medidas de Seguridad

Ejemplo de redacción

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

Medidas administrativas

1. Adopción de un esquema de capacitación permanente en materia de la Ley General de Protección de Datos Personales en posesión de Sujetos Obligados (LGPDPPSO), impartido mediante el Campus Virtual de Capacitación del organismo garante.
2. Implementación de formatos de entrada y salida de préstamo de documentos por parte del área encargada del archivo.
3. Resguardo de los expedientes bajo los criterios, directrices y lineamientos para la atención de los expedientes técnicos
4. Mecanismos de control desarrollados conforme a lo establecido en los lineamientos del Sistema de Gestión de Documentos institucional.
5. Suscripción de una carta responsiva por parte de los usuarios o personal con acceso a sistemas de datos personales, acerca del deber de confidencialidad.
6. Reportar al superior jerárquico los incidentes detectados respecto de pérdida o alteración de cualquier documento que contengan datos personales.

NOTA: Estas medidas de seguridad se presentan a manera de ejemplo, cada sujeto obligado integrará las correspondientes de acuerdo con su posibilidad y contexto, cuidando que representen metas alcanzables

Ejemplo de redacción

Medidas físicas

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

Medidas técnicas

1. Utilizar claves de usuario y contraseñas de manera personal, y evitar compartirlas, prestarlas o registradas a la vista de otras personas.
2. Establecer y utilizar contraseñas robustas, es decir, de al menos ocho caracteres alfanuméricos y especiales, evitando que sean iguales al nombre del usuario, o cualquier otro nombre de personas, considerando que éstas sean fáciles de recordar y difíciles de adivinar o descifrar por un tercero, a fin de salvaguardar la información y datos personales a los que se tenga acceso.
3. Notificar de manera inmediata a la Dirección General de Sistemas los casos en los que los usuarios identifiquen o consideren que sus claves de usuario y/o contraseñas han sido utilizadas por un tercero.
4. Utilizar el correo electrónico para fines relacionados con las actividades laborales, evitando remitir datos personales.

NOTA: Estas medidas de seguridad se presentan a manera de ejemplo, cada sujeto obligado integrará las correspondientes de acuerdo con su posibilidad y contexto, cuidando que representen metas alcanzables

Ejemplo de redacción

5. Mantener los documentos electrónicos y físicos en lugares seguros, bajo llave, dentro de cajones cerrados, o bajo la protección de alguna contraseña, a fin de promover la restricción a los datos personales que pudieran contener.

6. No difundir, transmitir o compartir documentos electrónicos ni físicos que contengan datos personales, a fin de garantizar que estos no sean divulgados de manera no autorizada.

7. Evitar dejar u olvidar los documentos físicos que contengan datos personales en los equipos de impresión, así como evitar su impresión, escaneo y fotocopiado si no es realmente requerido para las actividades laborales.

8. Evitar el acceso a los sistemas de información de tratamiento de datos personales, bajo el precepto del mínimo privilegio; es decir, únicamente al personal que por sus funciones y facultades laborales los requiera, a fin de mantener una adecuada segregación de funciones, restricción de acceso y tratamiento de esos datos.

9. Borrar o eliminar de la papelera de reciclaje del escritorio de los equipos de cómputo los documentos o archivos electrónicos que nos son necesarios para el desarrollo de funciones.

10. Notificar las bajas de accesos a los sistemas de información o de tratamiento de datos personales, con oportunidad, para restringir el acceso a dichos datos por personal no autorizado

NOTA: Estas medidas de seguridad se presentan a manera de ejemplo, cada sujeto obligado integrará las correspondientes de acuerdo con su posibilidad y contexto, cuidando que representen metas alcanzables

Ejemplo de redacción

Adicionalmente, como parte de la política de seguridad técnica, la Dirección General de Sistemas implementa los siguientes controles:

1.Definición de políticas de contraseñas.

2.Asignación privilegios de acuerdo a roles y funciones.

3.Agente de seguridad instalado en administrativos de servidores de correo electrónico.

4.Tareas de respaldo por servidor y por agente.

5.Autenticación de correo electrónico.

6.Tareas de respaldo por servidor y de las instancias de base de datos del servicio.

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

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

9. Des habilitación de cuentas de personal que causa baja.

10. Acceso controlado de administración y accesos privilegiados.

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

NOTA: Estas medidas de seguridad se presentan a manera de ejemplo, cada sujeto obligado integrará las correspondientes de acuerdo con su posibilidad y contexto, cuidando que representen metas alcanzables

j) Monitoreo de las Medidas de Seguridad}

Ejemplo de redacción

La supervisión de las medidas de seguridad técnicas y físicas es un elemento importante para la mejora continua, pues permite definir nuevos controles de monitoreo y seguimiento de éstas. Entre las medidas de supervisión y monitoreo se encuentran las siguientes:

1. Revisar la actualización permanente del esquema de contraseñas conforme a las pantallas de parametrización de los sistemas, verificando que los valores se encuentren determinados conforme a la política.

2. Monitorear que todas las cuentas que se dan de alta para otorgar acceso a la red, sea validada en el campo correspondiente a la contraseña, a fin de asegurar el uso.

3. Revisar el cumplimiento de protocolos

k) Propuesta de Capacitación en Materia de Datos Personales

Ejemplo de redacción

La aplicación del programa de protección de datos personales en el ITAIPCH, requiere como un factor esencial, la formación y sensibilización de las personas que ahí laboran, de tal forma que pueda garantizarse la actualización y mejora continua del inventario de datos personales, la observancia de la normatividad y Ley, por lo que se propone un programa de capacitación en el tema de protección de datos personales que favorezca la profundización en el conocimiento del tema por parte de quienes intervienen en el tratamiento de datos personales.

A manera de propuesta, se han considerado los siguientes temas:

I) La Ley de protección de datos personales en posesión de sujetos obligados en Chiapas.
- Antecedentes
- Principios.
- Alcances
- Objetivo
- Implicaciones

II) Obligaciones en la observancia de la LPDPPSOCHIS
- Deberes.
- Medidas de seguridad.
- Procedimientos y sanciones/ Derechos ARCO (acceso, rectificación, cancelación y oposición).
- Medios de defensa.

III) El programa de protección de datos personales
- Sistemas de datos personales.
- Inventario y Base de Datos.
- Medidas de seguridad.
- Análisis de brecha y de riesgo.
- Funciones y obligaciones.

IV) El principio de información: Avisos de Privacidad en el marco del programa de protección de datos personales.
- Contenido: Integral, simplificado
- Consentimiento.
- Deber de información.
- Finalidades del tratamiento de los datos

INSTITUTO DE TRANSPARENCIA
ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES
CHIAPAS TRANSPARENTE

INSTITUTO DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES DEL ESTADO DE CHIAPAS

12ª. Poniente norte No. 1104. Colonia el Mirador

Tuxtla Gutiérrez, Chiapas

Tel. 961 550 0760

http://itaipchiapas.org.mx/

ESCUELA DE TRANSPARENCIA
Y FORMACIÓN CIUDADANA
ITAIP CHIAPAS

Escuela de Transparencia y Formación Ciudadana

Tel. 961 550 0748
Correo electrónico: capacitacioniaipchiapas@gmail.com
capacitación@itaipchiapas.org.mx
http://transparenciachiapas.org/capacitacion/