DOCUMENTO DE SEGURIDAD

DIRECCIÓN GENERAL DE PREVENCIÓN Y AUTORREGULACIÓN

AGENDA

Horario: 10:00 a 13:00 horas

Receso: Dos descansos de 15 minutos, cuando lo autorice el instructor

Agenda:

1. Contenidos del Documento de Seguridad
    1.1. Inventario de datos personales
    1.2. Funciones y obligaciones de las personas que traten datos personales.
    1.3. Análisis de riesgos
    1.4. Análisis de brecha
    1.5. Plan de trabajo
    1.6. Mecanismos de monitoreo y revisión de las medidas de seguridad
    1.7. Programa general de capacitación

2. Actualización.

SEGURIDAD DE LA INFORMACIÓN

MEDIDAS DE SEGURIDAD

LGPDPPSO

Artículo 31. Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las **medidas de seguridad** de carácter **administrativo**, **físico** y **técnico** para la protección de los **datos personales**, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su **confidencialidad, integridad y disponibilidad**.

Artículo 32. Las medidas de seguridad adoptadas por el responsable deberán considerar:

- El riesgo inherente a los datos personales tratados;
- La sensibilidad de los datos personales tratados;
- El desarrollo tecnológico;
- Las posibles consecuencias de una vulneración para los titulares;
- Las transferencias de datos personales que se realicen;
- El número de titulares;
- Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
- 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.

MEDIDAS DE SEGURIDAD LPDPPSOQR

Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Quintana Roo Arts. 32 y 33

Artículo 32. Con independencia del tipo de sistema en el que se encuentren los Datos Personales o el tipo de Tratamiento que se efectúe, el Responsable deberá **establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los Datos Personales**, que permitan protegerlos contra d**año, pérdida, alteración, destrucción o su uso, acceso o Tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad**.

Artículo 33 Las medidas de seguridad adoptadas por el responsable deberán considerar:

- El riesgo inherente a los datos personales tratados;
- La sensibilidad de los datos personales tratados;
- El desarrollo tecnológico;
- Las posibles consecuencias de una vulneración para los titulares;
- Las transferencias de datos personales que se realicen;
- El número de titulares;
- Las vulneraciones previas ocurridas en los sistemas de tratamiento, y
- 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.

CONFIDENCIALIDAD

- Propiedad de la **información** que refiere a **no estar a disposición o ser revelada** a personas no autorizadas.
- Prevenir la divulgación no autorizada de información.

DISPONIBILIDAD

- Propiedad de un **activo** para ser **accesible y utilizable**.
- Controlar las interrupciones de los recursos.
- Prevenir interrupciones no autorizadas.

INTEGRIDAD

- La propiedad de salvaguardar **la exactitud y completitud de los activos.**
- Evitar la modificación no autorizada o accidental.

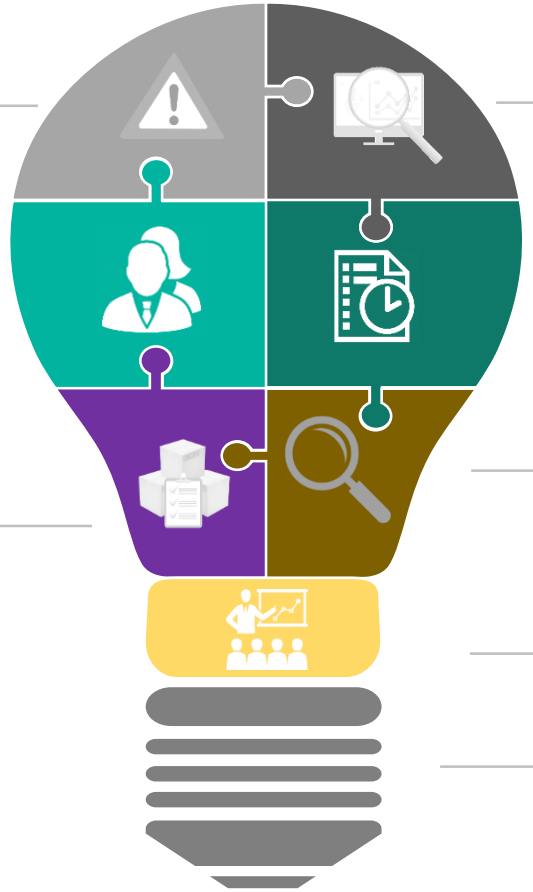
PROPIEDADES DE LA SEGURIDAD DE LA INFORMACIÓN

DOCUMENTO DE SEGURIDAD

Documento de seguridad

Artículos 35 de la LGPDPPSO y 37 de la LPDPPSOQR

Artículos 3 fracc. XIV de la LGPDPPSO y 4 fracc. XV de la LPDPPSOQR



Análisis de riesgos

Funciones y obligaciones

Inventario de datos personales

Análisis de brecha

Plan de trabajo

Mecanismos para monitoreo y revision medidas de seguridad

Programa general de capacitación

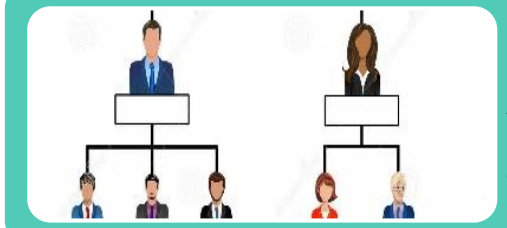
. Nombre y cargo del personal del Responsable o Encargado.

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

DOCUMENTO DE SEGURIDAD

PASO 1 – ELABORAR UN INVENTARIO DE DATOS PERSONALES Y SISTEMAS DE TRATAMIENTO

En este paso deberá identificar los tipos de datos personales que son tratados en los procesos y actividades de todas las áreas, asimismo, deberá indicar los sistemas de tratamiento físicos y electrónicos involucrados.



PASO 2 – ESTABLECER FUNCIONES Y OBLIGACIONES DE QUIENES TRATEN DATOS PERSONALES

A partir de la identificación de las actividades desarrolladas por el personal, deberá realizar una descripción de las actividades realizadas por perfil de puesto respecto al tratamiento de datos personales a fin de definir perfiles y privilegios que permitan asignar responsabilidades sobre el tratamiento de datos personales realizado.

PASO 3 – ELABORAR UN ANALISIS DE RIESGOS

En este paso, a partir del análisis de riesgos, conocerá las amenazas y vulnerabilidades que pueden afectar la seguridad de los datos personales que resguarda.

PASO 4 – ELABORAR UN ANALISIS DE BRECHA

En este paso identificará las medidas de seguridad físicas, técnicas y administrativas que tiene implementadas actualmente, asimismo, identificará las medidas de seguridad que requiere implementar en sus sistemas de tratamiento

PASO 5 – ELABORAR UN PLAN DE TRABAJO

Derivado del análisis de brecha, deberá elaborar un plan de trabajo que puntualice las actividades a realizar, el responsable que las va a implementar y el tiempo y recursos destinados a su realización

PASO 6 - ESTABLECER MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

Definirá los mecanismos para realizar una revisión periódica que permita identificar que las medidas de seguridad implementadas protegen los datos personales de manera adecuada.

PASO 7 – DESARROLLAR UN PROGRAMA GENERAL DE CAPACITACIÓN

En este paso deberá elaborar un plan que permita capacitar al personal involucrado en el tratamiento de datos personales a partir de la especialización requerida para cada tratamiento identificado.

1. ELABORAR UN INVENTARIO DE DATOS PERSONALES Y SISTEMAS DE TRATAMIENTO

INVOLUCRADOS EN EL TRATAMIENTO DE DATOS PERSONALES

Responsable del tratamiento

Sujeto Obligado que **DECIDE** sobre el tratamiento de los datos personales. Debe tomarse en cuenta que el SO son todas las UA que lo conforman y tratan DP.

Unidad de transparencia

- Dar trámite a las solicitudes de derechos ARCO.
- Asesorar a las áreas adscritas al Responsable en materia de protección de datos personales.

Oficial de PDP

Experto designado para asesorar, forma parte de la Unidad de Transparencia.

Comité de transparencia

- Aprobar, supervisar y evaluar las políticas, programas, acciones y demás actividades
- Coordinar, realizar y supervisar las acciones necesarias…

INVOLUCRADOS EN EL TRATAMIENTO DE DATOS PERSONALES

*No contemplado en las definiciones de la LPDPPSOEP, pero si mencionado como Tercero Receptor en el art. 97

Tercero

Persona física o moral, nacional o extranjera, distinta del titular, del responsable y del encargado

Encargado

Persona física o jurídica, que sola o conjuntamente con otras trate DP **A NOMBRE Y POR CUENTA** del responsable

*Relación establecida a través de un instrumento jurídico que acredite su existencia, alcance y contenido.

EL INVENTARIO DE TRATAMIENTOS COMO PARTE FUNDAMENTAL EN EL CUMPLIMIENTO DE UN DEBER Y UN PRINCIPIO

- Para el debido cumplimiento con las obligaciones establecidas en la LGPDPPSO, es fundamental que cada responsable ubique los tratamientos de datos personales, las unidades administrativas y el personal que lo realiza.

- El inventario inicia con la información básica de cada tratamiento de datos personales que se realiza en la institución.

- Este diagnóstico se facilita cuando quien trata datos personales identifica correctamente el uso de la información en cada uno de los procesos del responsable.

TRAZABILIDAD DEL TRATAMIENTO DE DATOS PERSONALES

- La trazabilidad es la capacidad de rastrear todos los procesos, identificando el origen y las diferentes etapas de un proceso de producción y distribución de bienes de consumo.

- Trasladado a la seguridad de los datos personales, es la capacidad de identificar de dónde vienen, así como quién ha tenido acceso a ellos, dónde se almacenan, quién, a quién y dónde se han realizado transferencias o remisiones, quien los ha alterado, y quién y cuándo los han eliminado.

- La trazabilidad es de gran importancia ya que permite a las organizaciones tener un control riguroso de los datos personales que tratan, así como evitar la imposición de sanciones, toda vez que, permite demostrar el cumplimiento normativo y definir estrategias necesarias para mitigar los riesgos detectados.

INVENTARIO DE DATOS PERSONALES

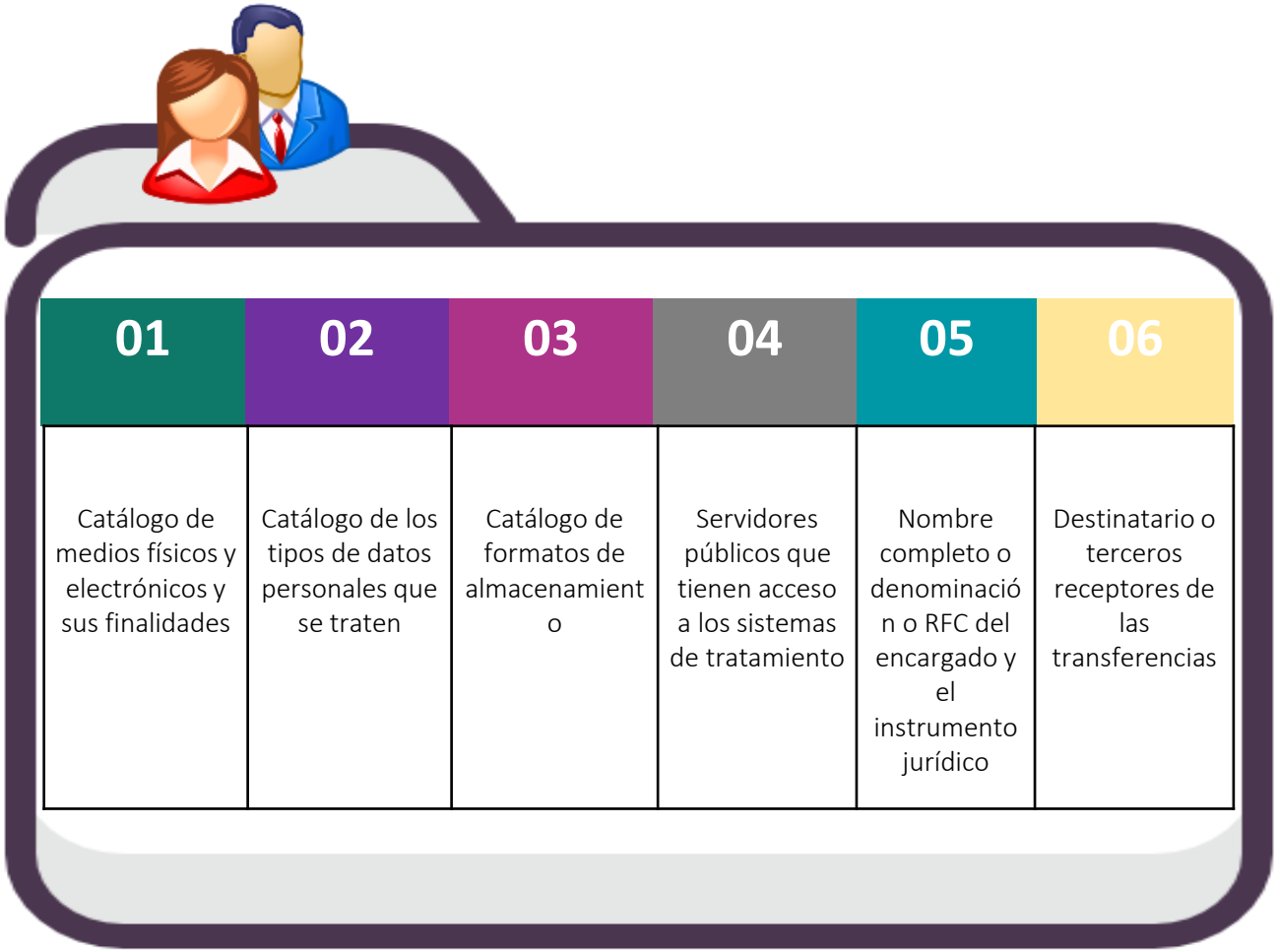
- Los elementos que debe incluir se definen en los Lineamientos Generales (Art. 58 y 59 de los Lin. Grales de PDP y art. 18, fracción III)

- Es responsabilidad del titular de cada unidad administrativa la información de los tratamientos declarada en el inventario.

INVENTARIO DE DATOS PERSONALES

Artículo 58 de los LGPDSP
Considerando al menos:

I. El catálogo de medios físicos y electrónicos por los que se obtienen los datos
II. Las finalidades de cada tratamiento
III. El catálogo de los datos personales que se traten
IV. El catálogo de formatos de almacenamiento
V. La lista de servidores públicos que tienen acceso
VI. En su caso el nombre completo del encargado, y el instrumento jurídico que formaliza la prestación de servicios
VII. Los destinatarios o terceros receptores de las transferencias



¿Cómo se elabora el inventario de tratamientos de datos personales?

El diagnóstico se puede elaborar en el archivo de Excel recomendado y su llenado puede facilitarse con el planteamiento de las siguientes preguntas:

1) ¿Qué tipo de datos personales recabo?

Para identificar qué tipo de datos personales se recaban en los distintos formatos que se utilizan y lo más importante preguntarse, si es necesario recabarlos o no. Esto con el fin de utilizar sólo los necesarios para el ejercicio de sus funciones.

2) ¿Cómo recabo esos los datos personales?

Para identificar en qué tipo de formatos se recaban y almacenan lo datos personales por el responsable.

3) ¿Dónde se almacenan los datos personales?

Cada formato identificado puede estar almacenado en una o más ubicaciones, físicas o electrónicas.

4) ¿Quién tiene permiso para acceder o manejar los datos personales?

Diferentes personas pueden tener acceso a los sitios donde se almacenan los datos personales, estás pueden tener permisos específicos.

CICLO DE VIDA DE LOS DATOS PERSONALES

Una vez situadas las circunstancias anteriores (art. 58 de los LGPDP)

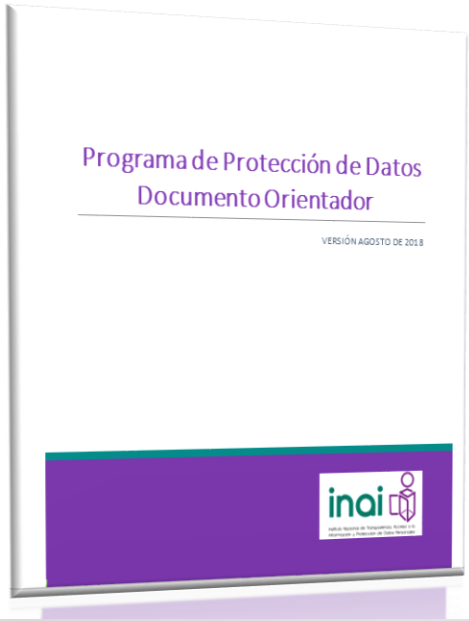
El responsable podrá ubicar y considerar el tratamiento de los datos personales **en el ciclo de vida de los datos.**

(art. 59 de los LGPDP)

INVENTARIO DE DATOS PERSONALES

- El INAI elaboró un Documento Orientador para la elaboración del Programa de Protección de Datos Personales, este se encuentran disponible en su página web junto con sus anexos

- El ANEXO1-InventariodeTratamientos corresponde a un ejemplo de inventario de tratamientos que los sujetos obligados pueden utilizar para la elaboración del propio.



inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

*Unidad Administrativa:	
*Fecha de elaboración o última actualización:	
*Nombre del tratamiento (proceso):	Señalar nombre del tratamiento.
*Fundamento jurídico que habilita el tratamiento:	Señalar las principales
*Atribuciones de la unidad administrativa para realizar el tratamiento:	Señalar las atribuciones específicas de la unidad administrativa para llevar a cabo el tratamiento, entre ellas, las que señala el Reglamento o Estatuto Orgánico interno, y otras si las hubiere.

Medio de obtención de los datos personales (1)			Tercero que transfiere los datos personales, en su caso (2)	Finalidades de la transferencia recibida, en su caso (3)	Listado de datos personales (4)		Sensible (5)	Formato de la base de datos (6)	
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.	Describir el medio, por ejemplo la fuente de acceso público, URL, domicilio, número telefónico, entre otros	En caso de seleccionar la opción otro, especificar el medio de obtención.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar el nombre del tercero o terceros que realizan la transferencia.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar para qué finalidades se realiza dicha transferencia. Se deberá utilizar la misma fila por tercero que transfiere.	Indicar cada uno de los datos personales que se tratan o sus categorías, uno por fila.	En caso de seleccionar la opción otro, especificar.	Señalar si el dato personal es sensible o no.	Señalar el o los formatos en los que se encuentra la base de datos del tratamiento.	Señ dat dat

Definición del proceso

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

*Unidad Administrativa:	
*Fecha de elaboración o última actualización:	
*Nombre del tratamiento (proceso):	Señalar nombre del tratamiento.
*Fundamento jurídico que habilita el tratamiento:	Señalar las principales disposiciones
*Atribuciones de la unidad administrativa para realizar el tratamiento:	Señalar las atribuciones específicas de la unidad administrativa para llevar a cabo el tratamiento, entre ellas, las que señala el Reglamento o Estatu

- Nombre de la Unidad Administrativa a cargo o administradora del proceso o procedimiento que trata los datos personales
- Fecha en que se concluye la elaboración del inventario
- Nombre del tratamiento (proceso)
- Fundamento jurídico del tratamiento (Facultades)
- Atribuciones de la unidad administrativa para realizar el tratamiento (Estatuto Orgánico)

Medios de obtención

Medio de obtención de los datos personales (1)			Tercero que transfiere los datos personales, en su caso (2)	Finalidades de la transferencia recibida, en su caso (3)
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.	Describir el medio, por ejemplo la fuente de acceso público, URL, domicilio, número telefónico, entre otros	En caso de seleccionar la opción otro, especificar el medio de obtención.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar el nombre del tercero o terceros que realizan la transferencia.	Si en la columna 1 se indicó que los datos personales se reciben por transferencia, señalar para qué finalidades se realiza dicha transferencia. Se deberá utilizar la misma fila por tercero que transfiere los datos personales.

- Medios de obtención de los datos personales (uno por fila)
- Medio por el cual se obtienen
- Si se declara que los datos fueron recibidos por transferencia se debe señalar al tercero que transfiere los datos
- Finalidad de la transferencia recibida

Tipos de datos personales

Listado de datos personales (4)		Sensible (5)
Indicar cada uno de los datos personales que se tratan o sus categorías, uno por fila.	En caso de seleccionar la opción otro, especificar.	Señalar si el dato personal es sensible o no.

- Listado de datos que se tratan en el proceso, ya sea por categorías o por datos.
- Identificación de tratamientos de datos personales sensibles

Categorías de datos personales

Datos personales	Categorías
• Nombre de persona física (titular de los datos personales, representante, tercero interesado, promovente, persona autorizada para recibir notificaciones, entre otros). • Año de nacimiento o edad • Correo electrónico personal • Creencias religiosas, filosóficas o morales • Currículum Vitae • Capacidades especiales • Domicilio • Estado de interdicción o incapacidad legal • Firma • Huella dactilar • Información genética • Información migratoria • Lengua indígena • Menor de edad • Nacionalidad • Nivel educativo • Ocupación • Opiniones políticas	• Antecedentes laborales • Beneficiarios • Características físicas • Circunstancias socioeconómicas • Datos académicos • Datos contenidos en declaraciones patrimoniales • Datos de identificación • Datos de salud • Datos laborales • Datos patrimoniales • Datos personales contenidos en documento para acreditar personalidad del representante • Datos personales contenidos en la descripción del trámite a realizar o solicitud de derecho a ejercer. • Datos personales contenidos en la identificación oficial presentada por la persona física • Datos sindicales • Datos sobre procedimientos judiciales o seguidos en forma de juicio • Descuentos personales (ahorro voluntario, hipoteca, seguro médico, seguro de automóvil, entre otros)

Sistemas de tratamiento

Formato de la base de datos (6)	Ubicación base de datos (7)		Sección de archivos (8)	Serie de archivos (9)	Subserie de archivos (10)
Señalar el o los formatos en los que se encuentra la base de datos del tratamiento.	Señalar la ubicación de la base de datos. Si es más de uno, se deberá indicar uno por fila.	En caso de seleccionar la opción otro, especificar la ubicación.	Indicar clave de identificación de la sección a la que corresponde el tratamiento.	Indicar clave de identificación de la serie a la que corresponde el tratamiento.	Indicar clave de identificación de la subserie a la que corresponde el tratamiento.

- Formato en que encuentra el archivo o la base de datos (físico, electrónico o digitalizado)
- Ubicación de la base de datos
- Información relacionada con archivos

Finalidades del tratamiento

Finalidades del tratamiento (11)
Indicar cada una de las finalidades del tratamiento, las cuales deberán ser explícitas y concretas. Una por fila.

- Descripción de las finalidades, asociadas al tratamiento (una por fila)

Consentimiento

¿Requiere consentimiento? (12)	Supuesto artículo 22 que se actualiza, en su caso (13)	Tipo de consentimiento (14)
Indicar si la finalidad requiere o no el consentimiento del titular.	En caso de que la finalidad no requiera el consentimiento del titular, señalar el o los supuestos del artículo 22 de la LGPDPPSO que se actualizan.	En caso de que la finalidad requiera el consentimiento del titular, señalar el tipo de consentimiento que se necesita.

- Identificar si para cada una de las finalidades declaradas si se requiere el consentimiento, en caso de NO ser requerido se debe incluir el supuesto del artículo 22 que es aplicable (excepciones al consentimiento).

Excepciones a consentimiento

Artículo 19 LPDPPSOQR

El responsable **no estará obligado a recabar el consentimiento** del titular para el tratamiento de sus datos personales en los siguientes casos:

1. Cuando una **ley** así lo disponga.
2. **Cuando las transferencias se realicen entre responsables, sean sobre datos personales que se utilicen para ejercicio de facultades compatibles o análogas con la finalidad que motivó su tratamiento.**
3. **Exista una orden judicial**, resolución o mandato fundado y motivado de autoridad competente;
4. Para el **reconocimiento o defensa de derechos** del titular ante autoridad competente;
5. Cuando los datos personales se requieran para **ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica** entre el titular y el responsable;
6. Exista **una situación de emergencia** que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
7. Los datos personales **sean necesarios** para la prevención, **diagnóstico,** la prestación de asistencia sanitaria
8. Los datos personales **figuren en fuentes de acceso público**;
9. Se sometan a un procedimiento de disociación.
10. Cuando los datos personales sea una persona reportada como desaparecida.

Responsabilidades del tratamiento

Servidores públicos que tienen acceso a la base de datos (15)	Área de adscripción (16)	Finalidad del acceso (17)
Señalar los puestos de los servidores públicos que tienen acceso a la base de datos del tratamiento correspondiente. Uno por fila.	Definir unidad administrativa a la que está adscrito el puesto	Señalar con qué fines tienen acceso los servidores públicos antes identificados. Uno por fila, según corresponda.

- Identificar los servidores públicos que tienen acceso a las bases de datos o archivos (registro por nombre de puesto)
- Incluyendo el área de adscripción
- La finalidad del tratamiento debe estar vinculado con la información del Manual de Organización de la Institución.

Remisiones

Nombre del encargado, en su caso (18)	No. de contrato, pedido o convenio con el encargado, o del instrumeto jurídico correspondiente (19)
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 número de identificación del instrumento jurídico que regula la relación con el encargado.

- Identificar los encargados y el instrumento jurídico correspondiente

(Art. 62 LGPDPPSO)

Transferencias

- Identificar si se realizan transferencias (artículos 65 a 70 LGPDPPSO)
- El tercero con quién se realiza la transferencia (uno por fila) (Artículo 3, fracción XXXII y artículo 65, de la LGPDPPSO)
- Identificar si la transferencia requiere consentimiento
- En caso de NO requerir consentimiento indicar los supuestos de los artículos 22, 66 y 70 de la LGPDPPSO aplicables
- Indicar el tipo de consentimiento que se requiere para cada finalidad (según aplica)
- Identificar si la transferencia requiere la suscripción de algún instrumento jurídico (artículo 66)

¿Se realizan transferencias? (20)	Tercero al que se transfieren los datos personales, en su caso (21)	Finalidades de la transferencia (22)	¿Requiere consentimiento la transferencia? (23)	Supuestos artículos 22, 66 o 70 que se actualizan, en su caso (24)	Tipo de consentimiento que se requiere para la transferencia (25)	¿La transferencia requiere la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico? (26)	Supuesto artículo 66 que se actualiza, en su caso (27)
Señalar si se realizan o no transferencias en el marco del tratamiento.	Señalar el nombre, razón o denominación social de los terceros a los que se transfieren los datos personales, cuando ello sea posible, o bien, su categoría. Uno por fila.	Señalar las finalidades para las cuales se transfieren los datos personales por cada uno de los terceros.	Señalar si la transferencia requiere o no consentimiento.	En caso de que la transferencia no requiera consentimiento, señalar los supuestos que se actualizan.	En caso de que la finalidad de la transferencia requiera el consentimiento del titular, señalar si se requiere el tácito o el expreso y por escrito.	Indicar si la transferencia requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico, según el artículo 66 de la LGPDPPSO.	Señalar el supuesto que en su caso se actualiza, si no se requiere de la suscripción de cláusulas contractuales, convenios de colaboración u otro instrumento jurídico.

Difusión

Difusión de los datos personales (28)	Fundamento jurídico para la difusión (29)
Indicar si en el tratamiento se realiza la difusión de los datos personales.	Indicar el fundamento jurídico que ordena la difusión de los datos personales.

- Identificar si se realiza una difusión de los datos personales.
- Fundamento jurídico para la difusión.

Plazo de conservación y bloqueo

- Definir los plazos de conservación de los datos personales (considerar lo establecido en los instrumentos de clasificación archivística).
- Identificar si se ha presentado algún bloqueo

Plazo de conservación (30)	Bloqueo (31)
Señalar el plazo de conservación de los datos personales, según lo señalado en los instrumentos de clasificación archivística.	PENDIENTE POR DEFINIR

2. ESTABLECER FUNCIONES Y OBLIGACIONES

ESTABLECER FUNCIONES Y OBLIGACIONES

Funciones y obligaciones de los que tratan datos personales

Identificar requerimientos específicos en materia de **capacitación** de DP.

Establecer **perfiles y privilegios** adecuados.

Establecer la **cadena de rendición de cuentas**, en caso de vulneraciones de seguridad.

Definir y documentar sus **funciones y obligaciones y los roles y responsabilidades**, respecto al tratamiento de los datos personales y los sistemas que los soportan.

Saber que **tipo de tratamiento** realiza con base al ciclo de vida de los datos.

Identificar al **personal** que realiza tratamiento de datos personales.

ESTABLECER FUNCIONES Y OBLIGACIONES DE QUIENES TRATEN DATOS PERSONALES

El sujeto obligado o responsable debe determinar y proveer los recursos (incluyendo humanos) para implementar, operar y mantener el Documento de seguridad, medidas de seguridad y el sistema de gestión de protección de datos personales.

Art. 57 de los LGPDSP

Para garantizar que la seguridad de los datos personales

a) Establecer y documentar roles y responsabilidades.

sea parte de los valores

b) Establecer la cadena de redición de cuentas.

institucionales

c) Asegurar que todos los integrantes del sujeto obligado conozcan tengan claras sus roles y funciones.

ESTABLECER FUNCIONES Y OBLIGACIONES DE QUIENES TRATEN DATOS PERSONALES

Recursos humanos parte de la organización

- Comunicar a todos los involucrados
- Roles y responsabilidades
- Contribución y consecuencias de incumplimiento

3. ELABORAR UN ANÁLISIS DE RIESGOS

¿QUÉ ES UN RIESGO?

Riesgo. Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para los titulares. Se relaciona con una ocurrencia que podría causar un resultado negativo, es una combinación de la probabilidad de un evento y su consecuencia desfavorable.

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

Identificar el riesgo. Proceso para encontrar, enlistar y describir los elementos del riesgo. Comprender los riesgos en términos de la misión del responsable es el primer paso para la gestión de los riesgos.

Riesgo de seguridad. Potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio del responsable y por lo tanto a titulares de los datos personales.

Amenaza: Circunstancia o condición externa, con la capacidad de causar daño a los activos (datos personales) explotando una o más de sus vulnerabilidades.

Vulnerabilidad: Circunstancia o condición propia de un activo, que puede ser explotada por una o más amenazas para causarle daño.

GESTIÓN DE RIESGOS

Gestión de riesgos. Es el proceso continuo de identificación de riesgos, su evaluación y a la creación de un plan para abordarlos.

Los riesgos se deben

- Identificar
- Comprender
- Evaluar
- Tratar

Así como sus vulnerabilidades subyacentes

Y, el impacto en la información-datos personales y sistemas que los soportan-titulares.

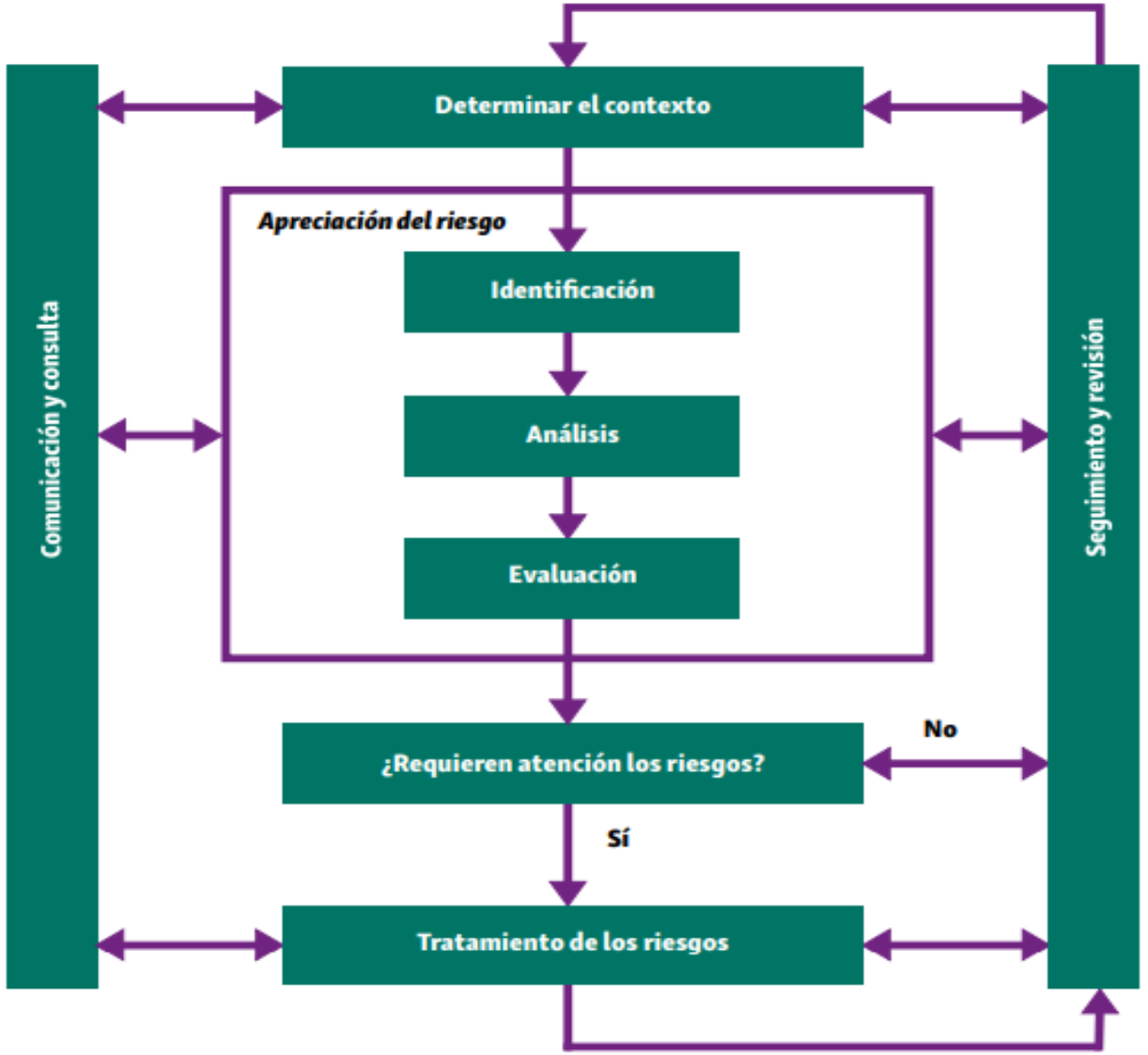
No existe la seguridad total o riesgo cero. Los riesgos y amenazas siempre existen, sin importar la cantidad de recursos que destine el responsable para su atención, por ello se debe realizar una gestión de riesgos acorde a los objetivos y capacidades del responsable.

La gestión de riesgos considera también determinar la tolerancia del responsable a ellos, estableciendo las opciones de tratamiento que se aplicará a cada riesgo.

El objetivo de la gestión de riesgos es mantenerlos debajo de la tolerancia establecida.

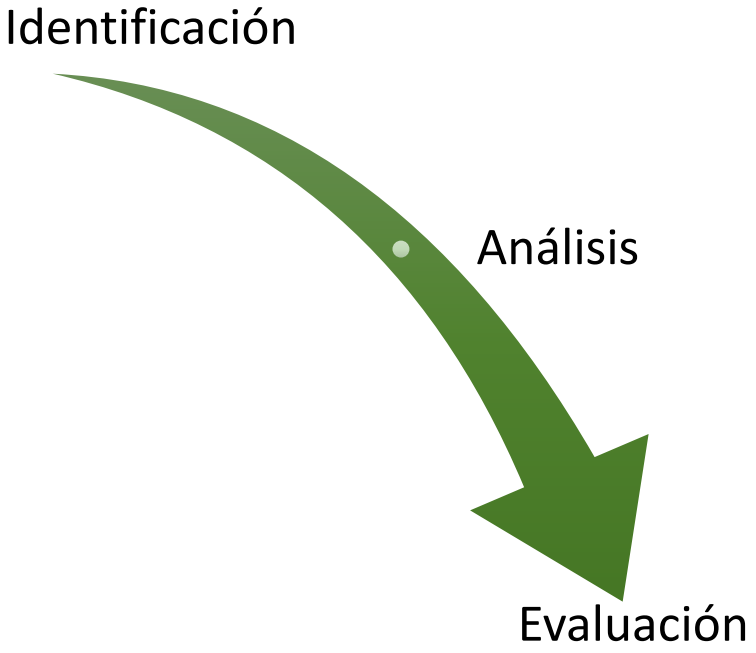
ESQUEMA GENERAL DE LA GESTIÓN DE RIESGOS

No debemos perder de vista que el análisis de riesgos se refiere a una actividad específica que cuenta con sus actividades propias y forma parte de la gestión de riesgos, es decir, el análisis de riesgos es una actividad que se encuentra dentro de un ciclo ligado a un proceso previo y es necesario para realizar un proceso posterior a partir de la interpretación de los resultados obtenidos, mismo que se encuentra ligado al tratamiento de riesgos que será detallado en el análisis de brecha.



EVALUACIÓN O APRECIACIÓN DEL RIESGO

La evaluación o apreciación del riesgo es un proceso que se centra en describir los riesgos a los que se enfrentan los activos a fin de obtener un resultado que sirva como indicador para la toma de decisiones y las acciones que se deben emprender para minimizar la materialización de un incidente de seguridad, por lo cual deberá realizar:



Identificación del riesgo

- En esta fase se busca encontrar, reconocer y describir los riesgos a los que se enfrentan los activos, buscando contestar a las preguntas ¿qué puede suceder? y ¿cómo puede suceder?

Análisis del riesgo

- Con el paso previo, se retoman los riesgos identificados, sus amenazas y vulnerabilidades, se determina la probabilidad de ocurrencia, las consecuencias de su materialización y finalmente a calcular el nivel de riesgo a partir de la integración de escenarios.

Evaluación del riesgo

- Para retomar en nivel de riesgo obtenido y comparar contra los criterios definidos de aceptación a fin de establecer prioridades para atender.

IDENTIFICACIÓN DEL RIESGO

A partir de la descripción de los activos, antes de iniciar el análisis de riesgos de datos personales, es necesario identificar peligros, considerando las amenazas y vulnerabilidades para los datos personales y los recursos involucrados en su tratamiento, los cuales pueden ser, de modo enunciativo mas no limitativo: hardware, software, personal del responsable, entre otros.

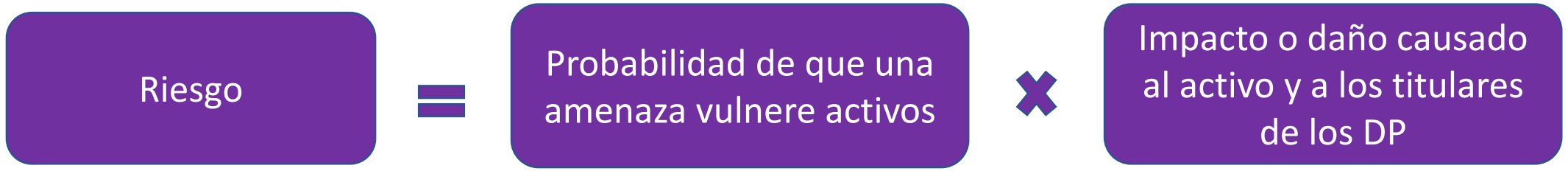
En otras palabras, la identificación de los riesgos busca relacionar las amenazas con vulnerabilidades para identificar el peligro al que se enfrenta el activo (el dato personal).

De esta manera, lo que se identifique será analizado en la siguiente etapa. Lo que no se identifique quedará como riesgo ignorado.

ANÁLISIS DE RIESGO DE LOS DATOS PERSONALES

Análisis de riesgo: Es el proceso para comprender la naturaleza del riesgo (peligro) y/o determinar su magnitud aceptable o tolerable. Consiste en averiguar el nivel de riesgo que el responsable o sujeto obligado está soportando. Para ello, tradicionalmente las metodologías proponen que se realice un inventario de activos, se determinen las amenazas, las probabilidades de que ocurran y los posibles impactos.

Los activos, las amenazas y las vulnerabilidades se combinan para generar riesgos. Cuando un riesgo se materializa, ocurre un incidente de seguridad, el cual se traduce en una violación a las medidas de seguridad.



METODOLOGÍAS

Los sujetos obligados deberán adoptar alguna metodología o a partir de alguna crear una propia para gestionar el riesgo.

Existen múltiples metodologías, entre las más comunes encontramos:

- **ISO 31000:2018 Gestión de riesgo – Directrices:** https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es
- **ISO 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks:** https://www.iso.org/standard/80585.html
- **MAGERIT v3:** https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Y_brBS9t_EY
- **NIST SP 800-30 "Guide for conducting risk assessments-** https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- **ENISA - Inventory of Risk Management / Risk Assessment Methods and Tools:** https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory

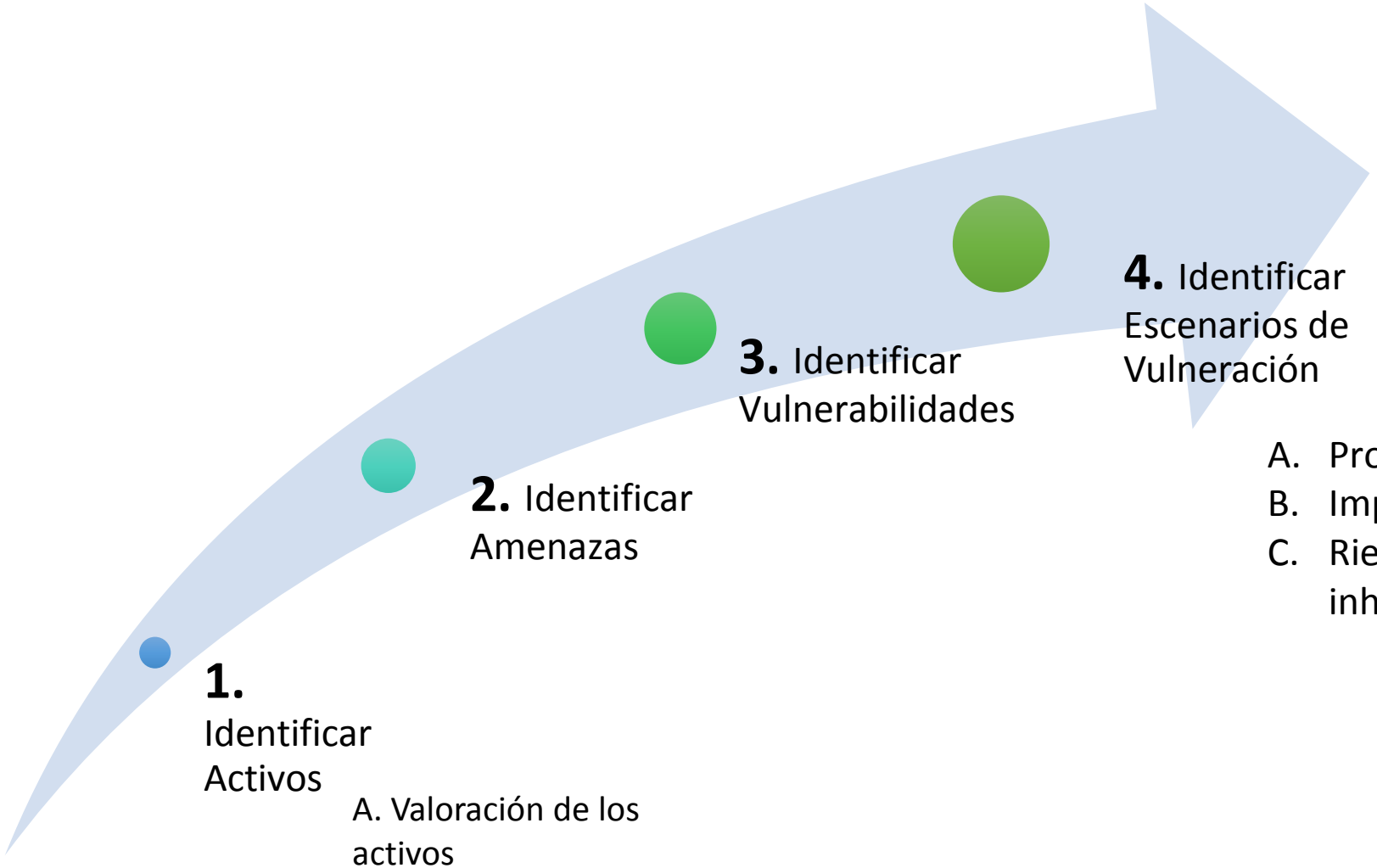
METODOLOGÍAS

El análisis de los riesgos busca calificar los riesgos identificados, a partir de la cuantificación de la probabilidad de ocurrencia y de sus consecuencias en términos de probabilidad y estadística (análisis cuantitativo), o bien, ordenando su importancia relativa (análisis cualitativo).

En este punto resalta la importancia de contar con una metodología, la cual se centra en brindar una visión estructurada que permita al interesado contar con una visión estructurada en preguntas o actividades definidas que den soporte a la asignación cuantitativa y/o cualitativa de los elementos que comprenden el riesgo.

Permitiendo así contar con un panorama reproducible para la valoración de los riesgos con el resto de los activos a valorar.

VALORACIÓN RESPECTO AL RIESGO



1. Identificar Activos

A. Valoración de los activos

2. Identificar Amenazas

3. Identificar Vulnerabilidades

4. Identificar Escenarios de Vulneración

A. Probabilidad
B. Impacto
C. Riesgo inherente

CRITERIOS DE EVALUACIÓN

Considerar los del artículo 32 de la LGPDPPSO

Tolerancia= Nivel de Riesgo Aceptable

Probabilidad

Impacto

Daño a los titulares

Realizar el Análisis de Riesgo de los Datos Personales

- Identificar Activos

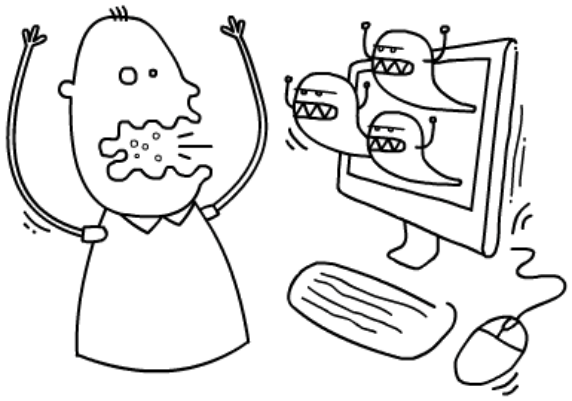
Activos de Información

Activos de Apoyo

Identificación de Activos de (ejemplo)

REALIZAR EL ANÁLISIS DE RIESGO DE LOS DATOS PERSONALES

- Identificar Amenazas



Amenazas de los Activos (ejemplo)

Fuego

Virus

Robo de información

Pueden ser de origen natural o humano, accidentales o deliberadas y además provenir de adentro o fuera de la organización.

REALIZAR EL ANÁLISIS DE RIESGO DE LOS DATOS PERSONALES

- Identificar Vulnerabilidades

Vulnerabilidades de los activos (ejemplo)

Falta de antivirus

Material susceptible al fuego

Las **vulnerabilidades** son *debilidades en los activos*

- Valoración de los activos

Se debe valorar cuantitativa y cualitativamente cada dimensión de seguridad. La escala de valor para cada propiedad será de 1 a 3, donde 1 es bajo, 2 es medio y 3 es alto, una vez determinados los valores individuales, se sumarán para obtener el valor total del activo, donde:

Valor cuantitativo	Valor cualitativo
1-3	Bajo
4-6	Medio
7-9	Alto

		Principios de la Seguridad			Valor del activo	
No.	Nombre del Activo	C	I	D		
1.	Sistema de expedientes clínicos	3	3	3	9	Alto
2.	CV	2	2	1	5	Medio
3.	Oficios	1	1	1	3	Bajo

- Identificar escenarios de Vulneración

Se deberá identificar la **probabilidad de que las amenazas exploten la vulnerabilidad de los activos, así como el impacto en los activos y en los titulares de materializarse dicha amenaza**.

Probabilidad

Se refiere a la posibilidad de que un evento ocurra en determinado periodo de tiempo, para asignar un valor a la probabilidad es necesario contar con la mayor información posible en función de diversos criterios, de manera enunciativa más no limitativa se pueden considerar los siguientes:

- Las medidas de seguridad implementadas
- Eventualidades conocidas
- Conocimientos del entorno
- Estadisticas

De esta manera, es posible determinar valores a la posibilidad de ocurrencia en una escala cuantitativa o cualitativa con elementos que sustenten el valor asignado.

- Criterios de Probabilidad

Se deberá identificar la **probabilidad de que las amenazas exploten la vulnerabilidad de los activos, así como el impacto en los activos y en los titulares de materializarse dicha amenaza**.

Probabilidad

Se refiere a la posibilidad de que un evento ocurra, considerando la cantidad de veces que podría presentarse en determinado periodo de tiempo, basándose en las eventualidades conocidas y el conocimiento del entorno. Por ejemplo:

Grado de Probabilidad		Criterio
Baja	1	Si ha ocurrido 1 antecedente registrado en un periodo de 5 años o y/o que por el entorno, la posibilidad de que suceda sea mínima.
Media	2	Si solo se han tenido 2 antecedentes registrado en un periodo anual y/o esporádicamente en un intervalo de 3 años, o que por el tipo de entorno y condiciones sea posible que ocurra.
Alta	3	Si ha habido más de dos eventos al término de un año o bien que por las condiciones actuales o el tipo de entorno sea sumamente posible que suceda.

Ejemplo:

Activo	Amenaza	Probabilidad	
		cuantitativa	cualitativa
Currículos vitae	Robo de información	2, puesto que se han registrado 2 antecedentes en un año.	Media
Currículos vitae	Incendio	1, no existe antecedente y es poco probable que ocurra.	Baja

Impacto:

Medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización.

El impacto deberá valorarse en una escala cualitativa y una cuantitativa y en las tres dimensiones de seguridad (en la confidencialidad, en la integridad y en la disponibilidad) se recomienda de 1 a 3, donde 1 es bajo, 2 es medio y 3 es alto.

Para obtener un valor único se estimará el promedio de las tres.

Finalmente, el promedio se valorará en la siguiente escala:

Valor objetivo	Valor subjetivo
1	Bajo
2	Medio
3	Alto

Debemos considerar que el impacto debe analizarse por cuanto a los daños o afectaciones a las personas titulares de datos personales, y no así la afectación a la organización, particularmente a su reputación, que si bien importa y afecta, no es el fin último y propósito del Documento de Seguridad, en tanto que se trata de la protección de un derecho fundamental.

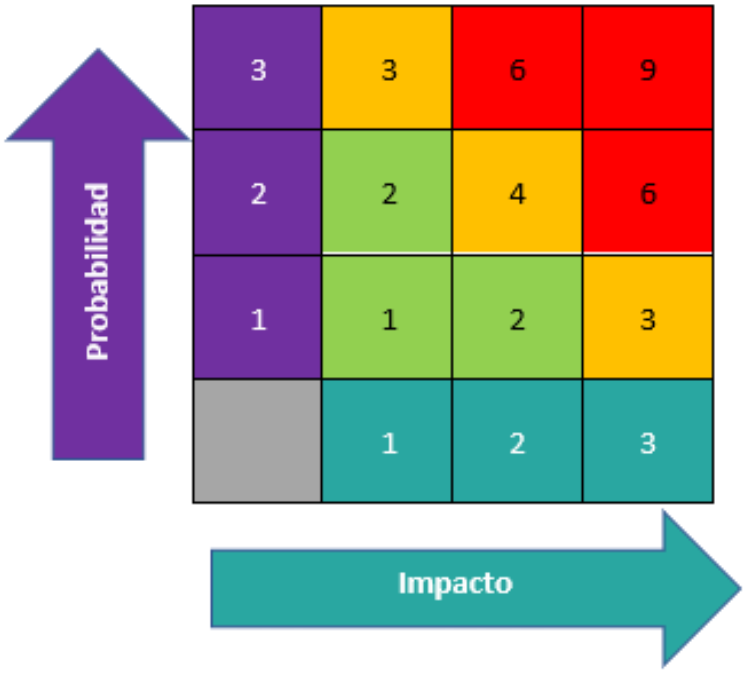
Ejemplo

Activo	Amenaza	Impacto				
					Impacto total	
		C	I	D	Valor cuantitativo	Valor cualitativo
Currículos vitae	Robo de información	2	2	1	1,6= 2	Medio
Análisis del impacto en los titulares: **De materializarse el riesgo "robo de documentos", los peores escenarios que pudieran observarse para los titulares son:** • **Daños en su integridad y seguridad en tanto que el CV contiene su dirección y teléfono particulares.** • **Pérdida de control de sus datos personales** **Problemas jurídicos en caso de que se modifiquen los datos sobre su historia académica o experiencia laboral.**						
Currículos vitae	Incendio	1	1	1	1	Bajo
Análisis del impacto en los titulares: **De materializarse el riesgo "incendio", no se considera que haya un impacto directo sobre los titulares, salvo causa de molestias en caso de tener que solicitarlos nuevamente.**						

Valoración del riesgo inherente:

Riesgo= probabilidad x impacto

Teniendo valores cualitativos y cuantitativos podemos valorar el riesgo, para ello podemos utilizar una matriz de riesgo o un mapa de calor, como el siguiente ejemplo:



Donde:

1-2= riesgo bajo

3-5= riesgo medio

6-9= riesgo alto

Así calculamos el riesgo intrínseco o inherente.

Para cada riesgo enumerado en la lista de amenazas, debemos realizar esta valoración

Ejemplo:

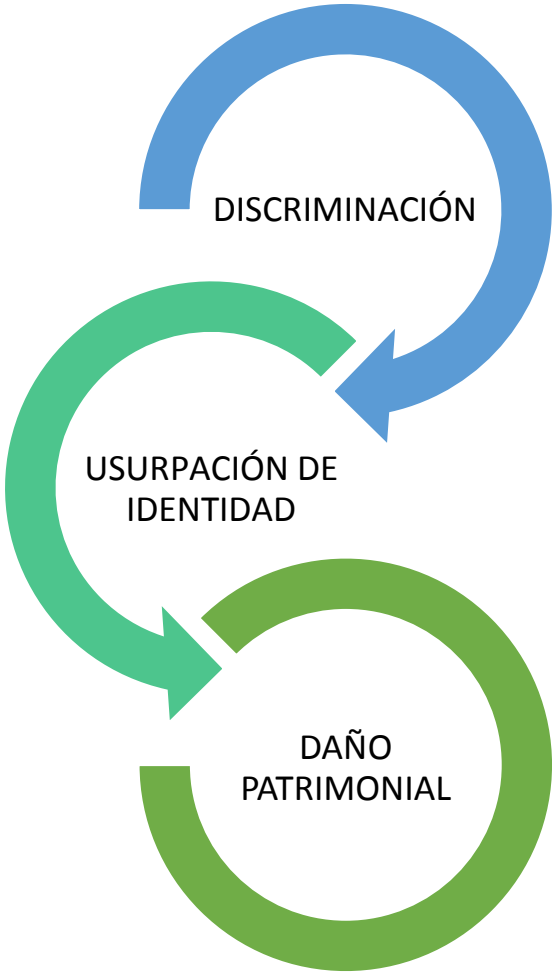
Activo	Amenaza	Probabilidad	Impacto	Riesgo inherente
Currículo vitae	Robo de datos	2-media	2-medio	4= Medio
Análisis de impacto en los Titulares: • Daños en su integridad y seguridad en tanto que el CV contiene su dirección y teléfono particulares. • Pérdida de control de sus datos personales • Problemas jurídicos en caso de que se modifiquen los datos sobre su historia académica o experiencia laboral.				
Currículo vitae	Incendio	1-baja	1-bajo	1=Bajo
Análisis de impacto en los titulares: De materializarse el riesgo “incendio”, no se considera que haya un impacto directo sobre los titulares, salvo causa de molestias en caso de tener que solicitarlos nuevamente.				

Si nuestro nivel de riesgo aceptable es bajo, el riesgo incendio, al ser bajo, no tiene prioridad para ser tratado, contrario al robo de datos, que tiene prioridad, en este caso.

ANÁLISIS DE RIESGOS
ART. 60 LINEAMIENTOS GENERALES

Para el análisis de riesgos el responsable deberá considerar :

1) Los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico;
2) El valor de los datos personales de acuerdo a su clasificación previamente definida y su ciclo de vida;
3) El valor y exposición de los activos involucrados en el tratamiento de los datos personales;
4) Las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida, y
5) Los factores previstos en el artículo 32 de la Ley General.



4. ELABORAR UN ANÁLISIS DE BRECHA

DEFINICIÓN DEL ANÁLISIS DE BRECHA

El **análisis de brecha** consiste en identificar:

- Las medidas de seguridad **existentes**
- Las medidas de seguridad existentes que **operan correctamente**
- Las medidas de seguridad **faltantes**
- Si existen **nuevas medidas de seguridad** que puedan reemplazar a uno o más controles implementados actualmente.

Las metodologías para la implantación de Sistemas de Gestión de Seguridad de la información incorporan catálogos de controles o medidas de seguridad, como la ISO 27002 o bien el de MAGERIT, por ejemplo.

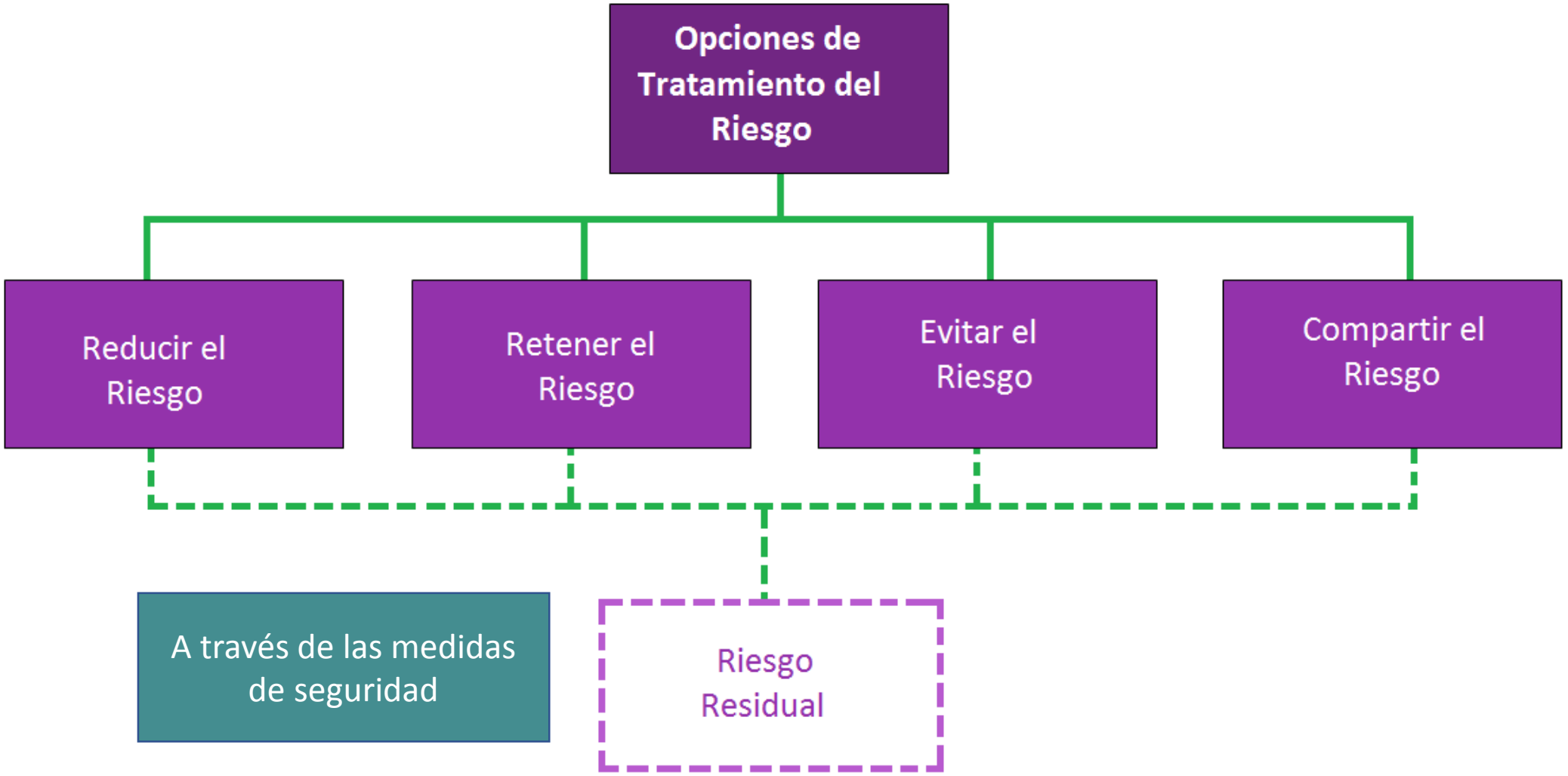
Artículo 33 fracción V de la LGPDPPSO y 61 de los Lineamientos Generales.

ANÁLISIS DE BRECHA

Debemos comprender que **el análisis de brecha está estrechamente relacionado con el análisis de riesgos**, se requiere del análisis de riesgos para proceder al análisis de brecha, **las fracciones del artículo 35 están en un orden elocuente de acuerdo a un Sistema de Gestión de Seguridad de Datos Personales, y es de suma importancia que se realicen en ese orden**.

El **análisis de riesgos sirve para visualizar qué activos tenemos, sus amenazas y los riesgos**, una vez que se ha evaluado el riesgo estamos preparados para tomar mejores decisiones, **revisar nuestras medidas de seguridad, controles o salvaguardas ya implementadas, si están funcionando para reducir el riesgo, y cuáles más podemos implementar**. En otras palabras, a partir de la interpretación de los resultados obtenidos del análisis de riesgos, se deberán seleccionar e implementar las medidas de seguridad administrativas, técnicas o físicas orientadas a cumplir con el objetivo fijado para los riesgos.

Tratar el Riesgo



- **Reducir el Riesgo.** Corrección, eliminación, prevención, minimización del impacto, disuasión, recuperación, monitoreo y concienciación.

- **Retener el Riesgo.** Aceptación de la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido, y se recomienda implementar medidas de seguridad en cuanto sea posible.

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

- **Compartir el Riesgo.** Un tercero interviene para mitigar los posibles efectos de un riesgo.

Se comparte el riesgo, pero no la responsabilidad

- **Aceptar el Riesgo.** Asumir formalmente algunos riesgos, coexistir con ellos, lo que requerirá aceptación formal del responsable del tratamiento.

Objetivo del análisis de brecha

El análisis de brecha es una actividad que permite complementar el ciclo de la gestión del riesgo, se determina que el resultado de esta actividad busca establecer prioridades de tratamiento de riesgo a partir su identificación, por lo que, podemos describir tres actividades que integran el análisis de brecha:

1. Como identificador de si se cuenta o no con una o varias medidas de seguridad físicas, técnicas y administrativas orientadas a mitigar el riesgo analizado sin describir su eficacia.

2. Se refiere a una valoración que describa la eficacia del control implementado al asociar la medida con la modificación del nivel de riesgo.

3. Determinar a partir de la descripción de la o las medidas de seguridad observadas el nivel de madurez que se tiene.

ANÁLISIS DE BRECHA

Estas acciones estan orientadas a trabajar con medidas de seguridad especificas para el tratamiento de los riesgos, lo que puede incluir la implementación de nuevos controles de seguridad o la actualización de los controles existentes.

1º. Identificación de las medidas de seguridad

En esta etapa se debe identificar si se cuenta o no con controles de seguridad de los riesgos identificados, se recomienda contar con un documento comparativo que ayude a identificar diversos controles de seguridad que permita atender de mejor manera los riesgos (por ejemplo la metodología utilizada).

2do. Valoración de la medida

En este paso se valora si el control identificado mitiga el riesgo de alguna manera, es decir, se procede a hacer una nueva valoración del riesgo en las condiciones definidas en el análisis de riesgos pero ahora con nuevos elementos que permiten determinar la disminución del riesgo en probabilidad o impacto.

3º. Nivel de madurez

En esta etapa se detalla el nivel de madurez de un control, es decir, se cuenta con un indicador que mide el grado en que el control está implementado y se ha integrado, para este paso se puede utilizar una escala a partir de la documentación obtenida por la implementación de los controles.

VALORACIÓN DE LAS MEDIDAS DE SEGURIDAD

Ahora que se tienen identificadas las medidas de seguridad, es necesario realizar una nueva valoración del riesgo, es decir, se debe volver a realizar el cálculo del riesgo en el contexto en el que este puede materializarse, solo que ahora en ese análisis se va a integrar como nuevo elemento la medida de seguridad a fin de identificar si esta reduce o no el valor calculado.

Este proceso permitirá identificar sin detallar si es que la medida realmente puede reducir el riesgo o no, lo anterior para definir la actualización o no de las medidas de seguridad.

NIVEL DE MADUREZ DE LAS MEDIDAS DE SEGURIDAD

La evaluación del nivel de madurez de una medida de seguridad es importante para identificar las áreas que requieren mejoras, medir la efectividad de la medida de seguridad y tomar decisiones informadas sobre cómo mejorar.

El nivel de madurez se puede evaluar utilizando una escala de madurez de 6 niveles, que es comúnmente utilizada en la gestión de la seguridad de la información:

- **Inexistente**. No se encuentra implementado
- **Inicial**: Se han implementado bajo una necesidad específica y ocasional sin evidencia documentada.
- **Repetible:** Se han implementado y existe un procedimiento, pero no están completamente documentados.
- **Definido:** Se han implementado y documentado totalmente en procedimientos, políticas y estándares.
- **Gestionado:** El control ha sido medido y monitorizado de manera regular para asegurar su eficacia y eficiencia.
- **Optimizado:** El control ha sido optimizado y mejorado continuamente para adaptarse a las necesidades cambiantes de seguridad.

TIPOS DE CONTROLES DE SEGURIDAD DE ACUERDO A SU FUNCIÓN

Disuasivos

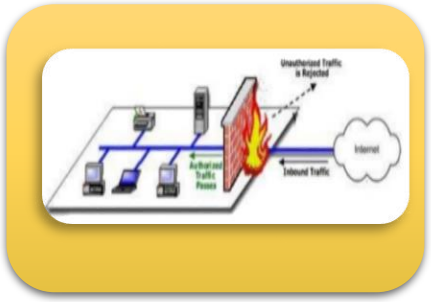
Reducen la posibilidad de un daño deliberado.
Ej. Implementación de procedimientos disciplinarios.

Preventivos

Anticipan la ocurrencia de fallas y reducen el impacto de una vulneración de seguridad
Ej. Control minimización de datos o anonimización desde el diseño del sistema

Correctivos

Reducen el efecto de una vulneración de seguridad ocurrida. (estas pueden disminuir impacto o probabilidad posterior al evento)
Ej. Recopilación de evidencia ante una vulneración.



Detectivos

Descubren la causa de fallas o vulneraciones de seguridad y disparan controles preventivos o correctivos.
Ej. Sistemas IDS y Antivirus.

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS

Ejemplo de Manual_Seguridad_Mipymes(Julio2015).pdf (inai.org.mx)

Análisis de Brecha (Medidas de seguridad existentes VS medidas de seguridad faltantes)				
Código	Pregunta o Control	¿Existente?		
		Sí	No	Observaciones
A.	Medidas de seguridad basadas en la cultura del personal			
A.1.	¿Pones atención en no dejar a la vista información personal y llevas registro de su manejo?			
A.1.1.	Política de escritorio limpio			
A.1.2.	Hábitos de cierre y resguardo			
A.1.3.	Impresoras, escáneres, copiadoras y buzones limpios			
A.1.4.	Gestión de bitácoras, usuarios y acceso			

MEDIDAS DE SEGURIDAD FÍSICAS

Análisis de Brecha (Medidas de seguridad existentes VS medidas de seguridad faltantes)				
Código	Pregunta o Control	¿Existente?		
		Sí	No	Observaciones
B.	Medidas de seguridad en el entorno de trabajo físico			
B.1.	¿Tienes medidas de seguridad para acceder al entorno de trabajo físico?			
B.1.2.	Mantener registros del personal con acceso al entorno de trabajo			

MEDIDAS DE SEGURIDAD TÉCNICAS

Análisis de Brecha (Medidas de seguridad existentes VS medidas de seguridad faltantes)				
Código	Pregunta o Control	¿Existente?		
		Sí	No	Observaciones
C.	Medidas de seguridad en el entorno de trabajo digital			
C.1.	¿Tienes medidas de seguridad para acceder al entorno de trabajo electrónico?			
C.1.1.	Uso de contraseñas y/o cifrado			
C.1.2.	Uso de contraseñas solidas			
C.1.3.	Bloqueo y cierre de sesiones			
C.1.4.	Administrar usuarios y accesos			

ANÁLISIS DE BRECHA
Ejemplo

					Valores despues del tratamiento				
Evaluación del riesgo	Controles existentes (antes de su tratamiento)	Nivel de madurez de los controles existentes	Opción de tratamiento	Controles de seguridad para el tratamiento	Impacto	Probabilidad	Riesgo		Evaluación del riesgo (riesgo residual)
							Cuantitativo	Cualitativo	
9	Control de accesos definidos al Sistema X	1. Se aplica sin estar documentado ni formalizado	1. Reducir el riesgo	9.1.1 Política de control de acceso	3	2	6	Alto	Riesgo no aceptable
9	Control de accesos definidos al Sistema X	1. Se aplica sin estar documentado ni formalizado	1. Reducir el riesgo	9.2.1 Registro y cancelación de usuarios	3	1	3	Medio	Riesgo no aceptable
9	Control de accesos definidos al Sistema X	1. Se aplica sin estar documentado ni formalizado	1. Reducir el riesgo	• Disociación y Separación	2	1	2	Bajo	Riesgo aceptable

Será importante que se defina **quién o quiénes serán los responsables de fortalecer las medidas de seguridad existentes (aumentar su nivel de madurez) y/o de implementar las nuevas**. Esto será parte importante para la elaboración del **Plan de Trabajo.**

5. ELABORAR UN PLAN DE TRABAJO

PLAN DE TRABAJO PARA LA IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD FALTANTES

Plan de Trabajo

El plan de trabajo debe **reflejar los recursos disponibles, humanos, económicos, de conocimiento y de tiempo** con los que se cuenta.

Debe contener al menos:

- Las acciones prioritarias.
- El periodo en el que se pretende cumplir las acciones.
- Las personas encargadas de cumplir con las acciones.

Cumplimiento Cotidiano de Medidas de Seguridad, fortalecer las existentes

Plan de Trabajo para la Implementación de las Medidas de Seguridad Faltantes

- Cumplimiento Cotidiano de Medidas de Seguridad

Cumplir con las políticas día a día

Aprobación de procedimientos donde se traten DP

Actualizaciones normativas respecto al tratamiento de DP

Revisar que el SGSDP refleje los cambios relevantes en la organización

Plan de Trabajo

Art. 61 Lineamientos Generales

El plan de trabajo debe reflejar los recursos disponibles, humanos, económicos, de conocimiento y de tiempo con los que se cuenta. Debe contener al menos:

1
- Defina acciones a implementar.
- La selección de las acciones prioritarias.

2
- Ser acorde al resultado del análisis de riesgo y análisis de brecha.
- El periodo en el que se pretende cumplir esas acciones.

3
- Priorizar las medidas de seguridad más relevantes e inmediatas a establecer de acuerdo al nivel de riesgo.
- Los recursos humanos y materiales para el cumplimiento de las acciones.

6. ESTABLECER MECANISMOS DE MONITOREO Y REVISIÓN DE LAS MEDIDAS DE SEGURIDAD

MONITOREO Y SUPERVISIÓN
ART. 33 FRACC. VII y ART. 35 FRACC. VI LGPDPPSO

Art 33. Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:

(…)

VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, (…)

Art 35. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:

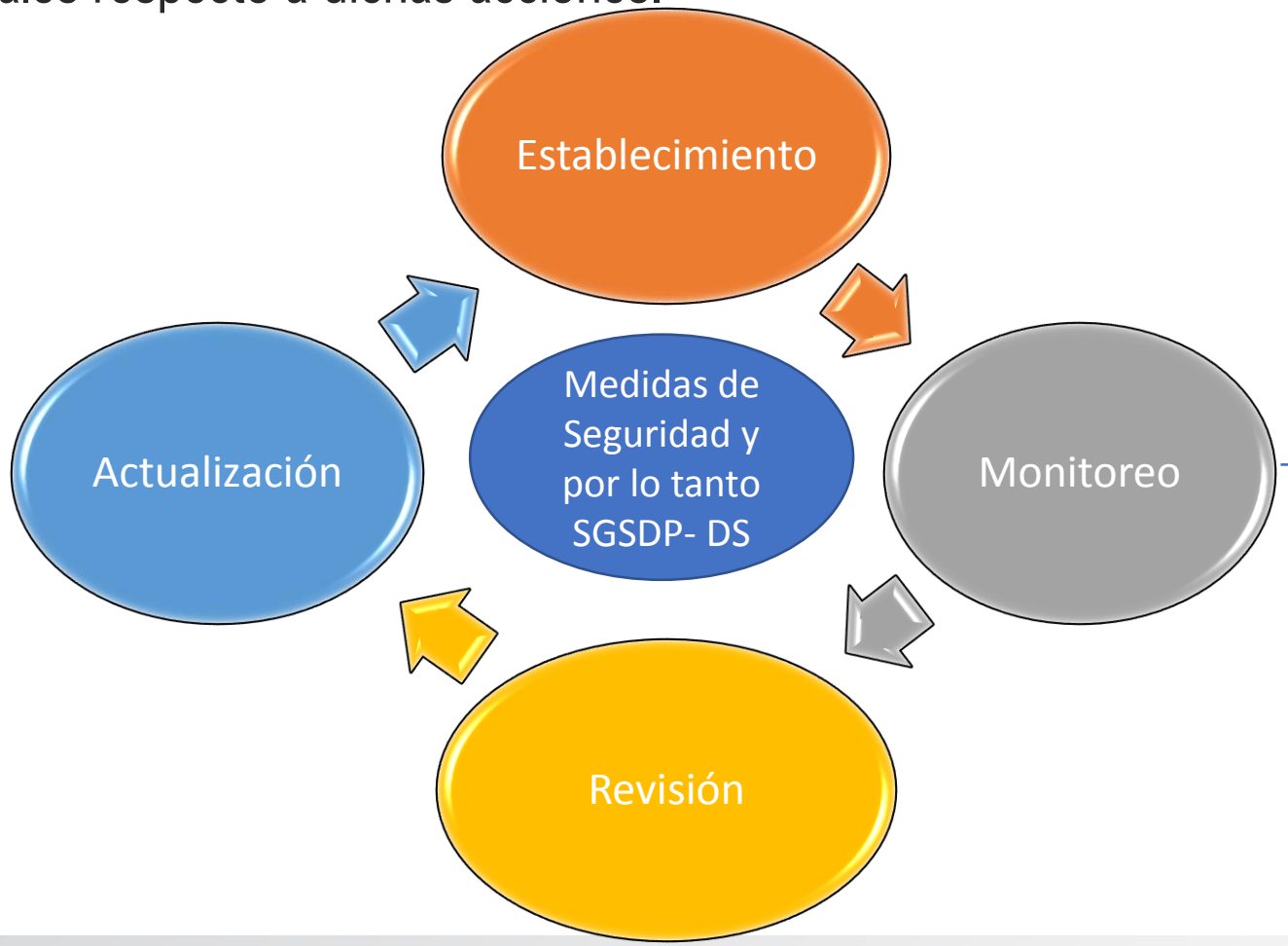
(…)

VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad,

(…)

MONITOREO Y SUPERVISIÓN

Debe comprenderse que, en materia de seguridad de los datos personales, el establecimiento, monitoreo, revisión y actualización debe verse como un proceso de mejora continua, en ese sentido se deben establecer las pautas generales respecto a dichas acciones.

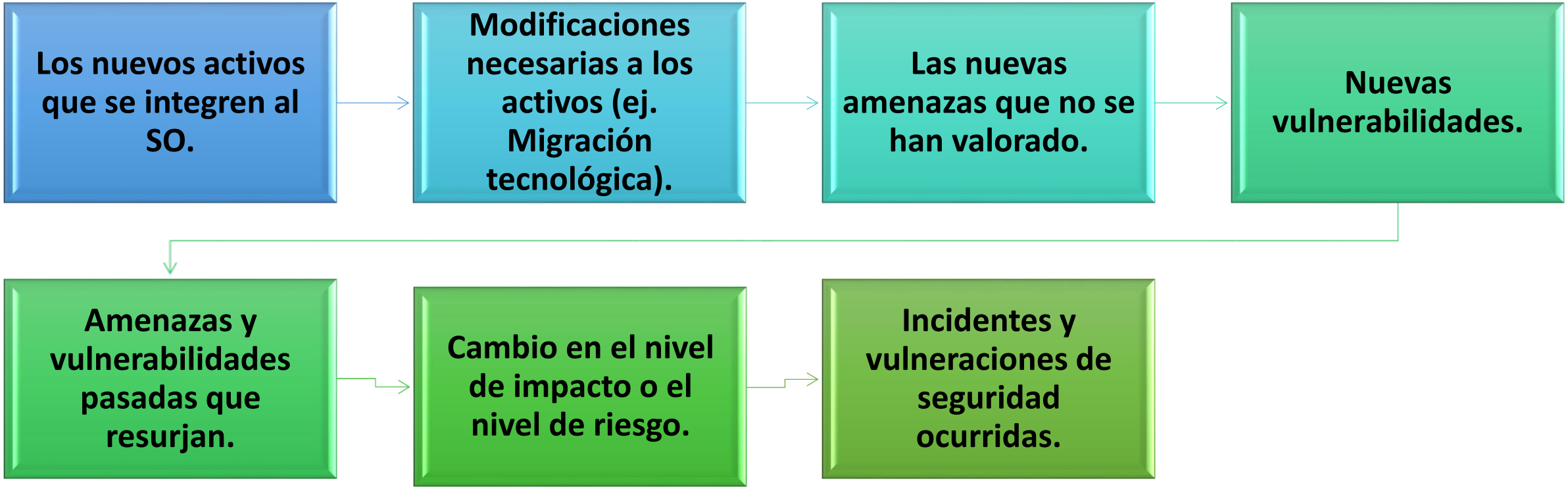


Monitoreo debe entenderse en dos partes:

1. monitorear riesgos.
2. Monitorear que las medidas de seguridad se estén aplicando y sean idóneas para el tratamiento del riesgo.

MONITOREO Y SUPERVISIÓN
ART. 63 LINEAMIENTOS GENERALES

El sujeto obligado deberá evaluar y medir los resultados de las medidas en materia de seguridad y tratamiento de los datos personales, a fin de verificar el cumplimiento de los objetivos propuestos e implementar mejoras de manera continua, para ello se deben monitorear constantemente:



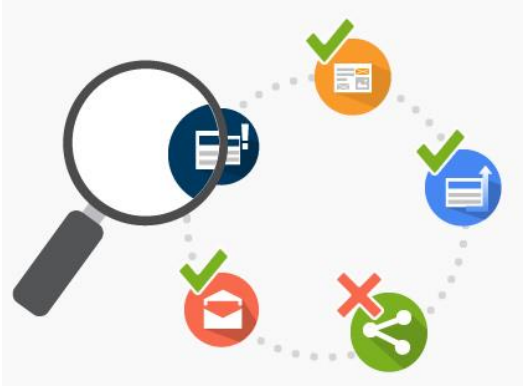
MONITOREO Y SUPERVISIÓN
ART. 63 LINEAMIENTOS GENERALES

Las revisiones y auditorías, así como diversos indicadores y alertas en el SGSDP, pueden avisar la ocurrencia de vulneraciones a la seguridad de los datos personales en cualquier fase del tratamiento.

Auditoría

Art. 63 último párrafo de los Lineamientos Generales. El responsable deberá contar con un programa de auditoría, interno y/o externo, para monitorear y revisar la eficacia y eficiencia del sistema de gestión.

Esta auditoría puede incidir en la actualización de las medidas de seguridad pero también en las fases del propio SGSDP.



AUDITORÍA VOLUNTARIA

Solicita

Responsables

Voluntariamente

Realiza

INAI

Organismos garantes

Objeto

Constatar adaptación, adecuación y eficacia

controles, medidas y mecanismos implementados

para cumplimiento de Ley y demás normativa

VULNERACIONES A LA SEGURIDAD

El sujeto obligado 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 organización debe identificar:
   a. Los activos afectados junto con el personal a cargo;
   b. Los titulares afectados;
   c. Las 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 debe comunicarse a los titulares de los datos personales, para que puedan tomar medidas que mitiguen o eviten una posible afectación.

3. Notificar a las autoridades de protección de datos y/o impartición de justicia, entre otras partes interesadas que pudieran auxiliar en el proceso de mitigar el incidente.

Registra Guardia Nacional, en tres años, 45 vulneraciones a sistemas

La **Sedena** notificó a la autoridad mexicana en protección de datos personales, el **Inai**, sobre la **vulneración a su sistema de correo electrónico**. La oficina de transparencia del **ejército mexicano** aseveró, según el oficio enviado al **Inai**, considera que la intromisión en su sistema de correo electrónico "no constituye una vulneración que afecte de forma significativa los derechos patrimoniales o morales de titulares de datos personales".

7. DESARROLLAR UN PROGRAMA GENERAL DE CAPACITACIÓN

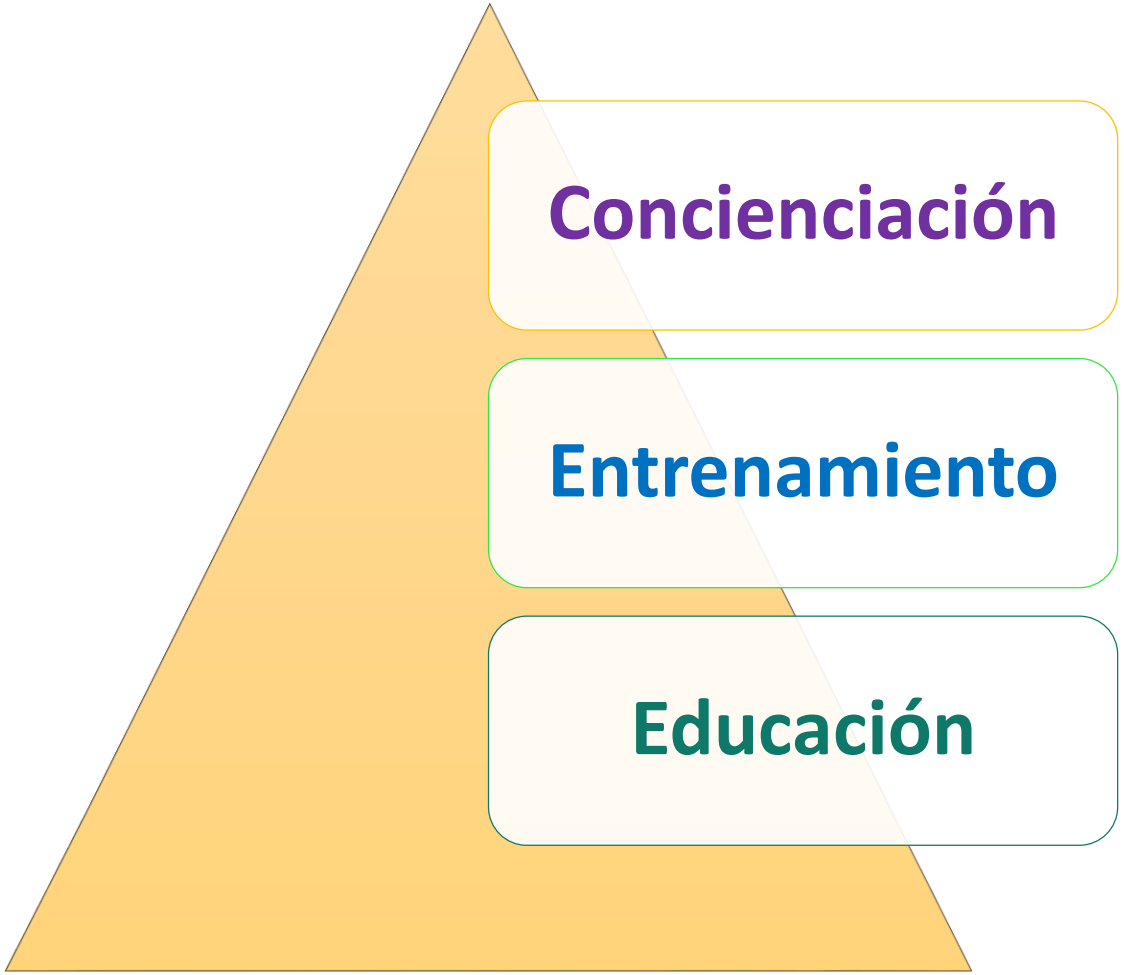
Capacitación

Art. 64 Lineamientos Generales

El sujeto obligado deberá diseñar e implementar programas a corto, mediano y largo plazo que tengan por objeto capacitar a los involucrados internos y externos en su organización, considerando sus roles y responsabilidades asignadas para el tratamiento y seguridad de los datos.

- Los requerimientos y actualización del sistema de gestión
- La legislación vigente en materia de protección de datos y las mejores prácticas
- Las consecuencias del incumplimiento de los requerimientos legales o requisitos organizacionales
- Las herramientas tecnológicas relacionadas o utilizadas para el tratamiento de los datos personales y para la implementación de las medidas de seguridad.

CAPACITACIÓN



Actualización del documento de seguridad

Documento de seguridad

¿CUÁNDO SE ACTUALIZA?

Cuando ocurran los siguientes eventos (Artículo 36 LGPDPPSO):

- Se produzcan **modificaciones sustanciales** al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
- Como resultado de un proceso de mejora continua, **derivado del monitoreo y revisión del sistema de gestión**;
- Como resultado de un proceso de mejora **para mitigar el impacto de una vulneración** a la seguridad ocurrida, y
- **Implementación de acciones correctivas** y preventivas ante una vulneración de seguridad.

¿QUÉ VA PRIMERO ?
DOCUMENTO DE SEGURIDAD VS SGSDP

- El Documento de seguridad se define como el instrumento que describe y da cuenta de modo general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee.

- El sistema de gestión se identifica como el 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 la Ley General y las demás disposiciones que le resulten aplicables en la materia.

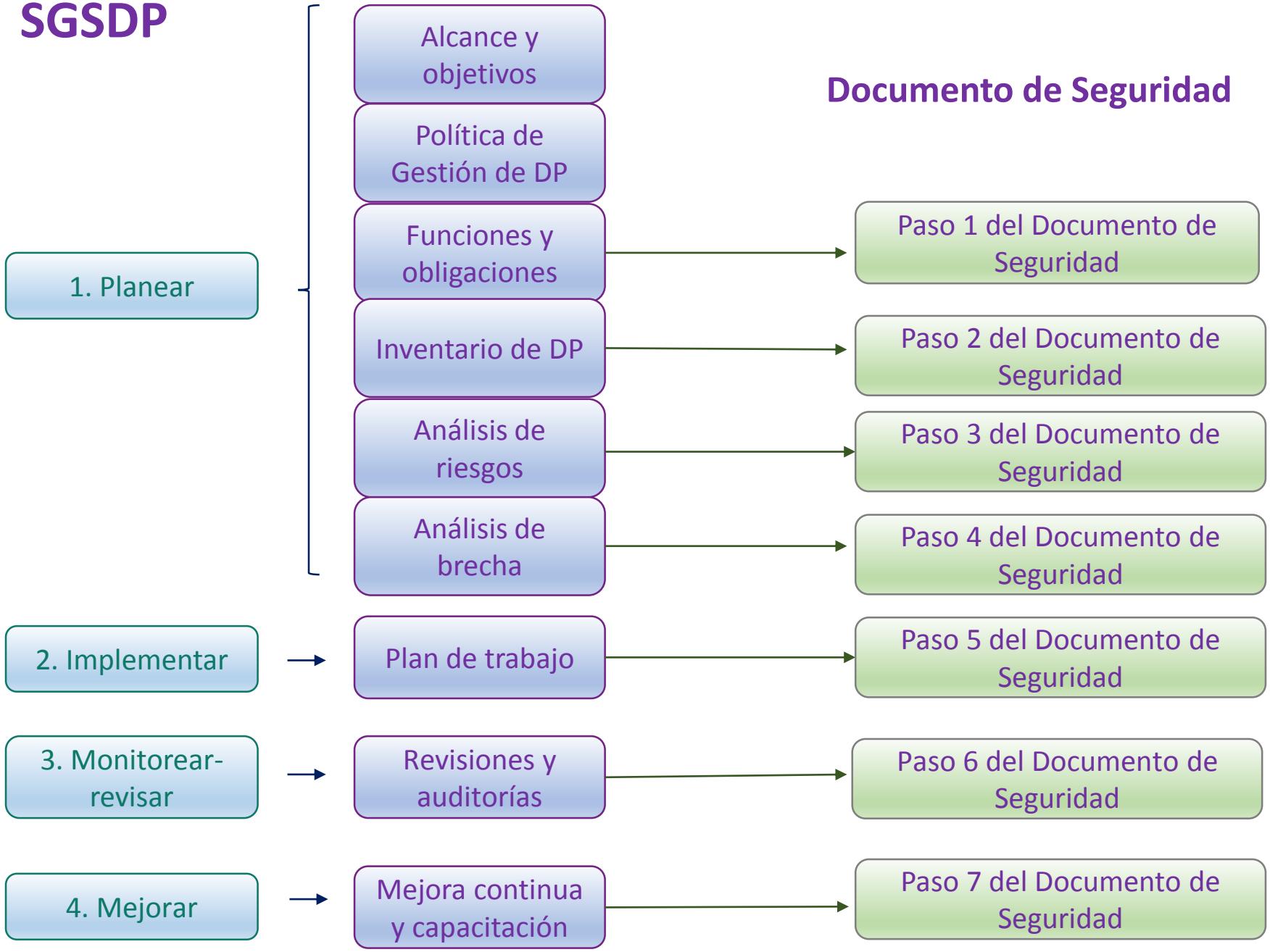
- El Documento de Seguridad puede ser creado en la fase de planeación previa a la de implementación del SGSDP

- Todas las medidas de seguridad implementadas por el Responsable deben documentarse en el Documento de Seguridad

- De este modo, puede apreciarse una clara relación entre la implementación de un sistema de gestión y la elaboración del Documento de seguridad, evidenciando que es necesario empatar los contenidos que se generan al llevar a la práctica un sistema de gestión y redactando el Documento de seguridad, pues son actividades que pueden ir de la mano, o bien elaborarse de modo independiente, buscando que exista una concordancia de contenidos que respalden las actividades que se realizan y documentan.

- La fase de planeación del SGSDP esta contenida en el documento de seguridad, a excepción de:
  - Elaboración de una política de gestión de datos personales.
  - Establecimiento del alcance y objetivos.

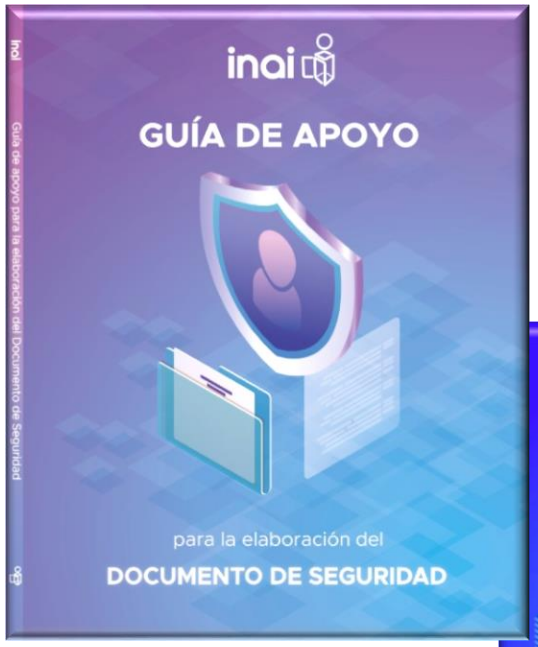
El documento de seguridad como base para Sistema de Gestión de Datos Personales



Conclusiones

1. El Documento de Seguridad es uno de los elementos para cumplir con el deber de seguridad.
2. Es indispensable que esto se realice con toda honestidad y lo más apegado a la realidad posible.
3. Deberá mantenerse siempre actualizado y ser de observancia obligatoria para todos los servidores públicos de las dependencias y entidades, así como para las personas externas.
4. Para identificar los tipos de datos personales que se tratan y los formatos en los que se encuentran, es necesario que cada una de las unidades administrativas realice un diagnóstico de los tratamientos de datos personales que llevan a cabo
5. A partir de su elaboración se tiene oportunidad de identificar a los servidores públicos que intervienen durante el procesamiento y aprovechamiento de los datos personales.

Materiales de utilidad (https://home.inai.org.mx/?page_id=3420)



CONVOCAN AL

PREMIO DE INNOVACIÓN Y BUENAS PRÁCTICAS EN LA PROTECCIÓN DE DATOS PERSONALES 2023

1 ¿QUIÉNES PUEDEN PARTICIPAR?

RESPONSABLES Y ENCARGADOS DEL SECTOR PÚBLICO Y PRIVADO, ASÍ COMO PÚBLICO EN GENERAL

UNIVERSIDADES. ESTUDIANTES Y PERSONAL DOCENTE DE NIVEL LICENCIATURA Y POSGRADO

2 ¿CÓMO PARTICIPAR?

IDEAS INNOVADORAS EN PROTECCIÓN DE DATOS PERSONALES, ATENDIENDO PRINCIPIOS, DEBERES U OBLIGACIONES

3 ¿BENEFICIOS?

FORTALECER CON INNOVACIONES LA PDP

PREMIOS EN EFECTIVO

PUBLICIDAD DEL GANADOR Y SU TRABAJO

RECONOCIMIENTOS

CONSULTA LAS BASES EN:
HTTPS://PREMIOINNOVACIONPDP.INAI.ORG.MX/

GRACIAS

DIRECCIÓN GENERAL DE PREVENCIÓN Y AUTORREGULACIÓN

Mtra. Mireya Arteaga Dirzo
Directora General de Prevención y Autorregulación
mireya.arteaga@inai.org.mx

Lic. Leticia Zamudio Cortés
Directora de Seguridad de Datos Personales del Sector Público
Correo electrónico: leticia.zamudio@inai.org.mx

Lic. María Fernanda Hernández Enríquez
Subdirectora de Seguridad de Datos Personales del Sector Público
Correo electrónico: fernanda.hernandez@inai.org.mx

Ing. Erwin F. Bautista Gaytán
Jefe de Departamento de Seguridad de Datos Personales del Sector Público
Correo electrónico: erwin.bautista@inai.org.mx