Se declara al año 2024, como "Año de Felipe Carrillo Puerto, Benemérito del Proletariado, Revolucionario y Defensor del Mayab".

Curso: Elaboración del Documento de Seguridad

DIRECCIÓN GENERAL DE PREVENCIÓN Y AUTORREGULACIÓN

BIENVENIDOS

Presentación.
Introducción a la Seguridad de la Información. Conceptos básicos.
Deber de seguridad
3. Documento de seguridad
  3.1. Inventario de datos personales.
  3.2. Funciones y obligaciones de las personas que traten datos personales.
  3.3. Análisis de riesgos
  3.4. Análisis de brecha
  3.5. Plan de trabajo
  3.6. Mecanismos de monitoreo y revisión de las medidas de seguridad
  3.7. Plan general de capacitación
Vulneraciones a la seguridad de los datos personales
Actualización del Documento de Seguridad.

LA RELACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN CON EL MARCO NORMATIVO PARA EL SECTOR PÚBLICO

Seguridad de la información

Es el conjunto de **medidas técnicas, organizativas y físicas que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de un sistema de información,**

Es proteger la información y los sistemas de información del acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados.

Deber de seguridad

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. (art. 31 Ley General) (Artículo 32 Ley local)

PROPIEDADES DE LA INFORMACIÓN

DISPONIBILIDAD

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

CONFIDENCIALIDAD

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

INTEGRIDAD

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

Deber de Seguridad

LGPDPPSO

Tipos de medidas de seguridad:

Adtvas.

- **Políticas y procedimientos** para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional. Ej. Capacitación y sensibilización

Físicas

- Acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados. Ej. Prevención de accesos no autorizados al perímetro de la organización, mantenimiento a los equipos.

Técnicas

- Acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los DP y de los recursos involucrados (activos). Ej. Prevención de accesos no autorizados a bases de datos y sistemas, esquema de privilegios para que el usuario realice sus actividades conforme a sus funciones.

Deber de Seguridad

LPDPPSOPEQR

Art. 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 daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.

Art. 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.

Actores que intervienen en la elaboración del Documento de Seguridad

INVOLUCRADOS EN EL TRATAMIENTO DE DATOS PERSONALES

Responsable

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.

Propietario

Persona servidora pública que tiene a cargo la ejecución de un proceso que involucra el tratamiento de datos personales. Tiene cargo de mando dentro de la estructura, por ejemplo el Director General de Recursos Humanos y Administrativos.

Encargado

Persona física o jurídica, pública o privada, ajena a la Org. del responsable, que sola o conjuntamente con otras trate DP A NOMBRE Y POR CUENTA del responsable

Oficial de PDP

Experto designado para realizar funciones del artículo 85 de la LGPDPPSO, está adscrito a la Unidad de Transparencia.

Custodio

Persona servidora pública con responsabilidad funcional sobre los activos, como: los responsables del departamento de datos, administradores de sistemas o responsables de un proceso o de un proyecto en específico, entre otros.

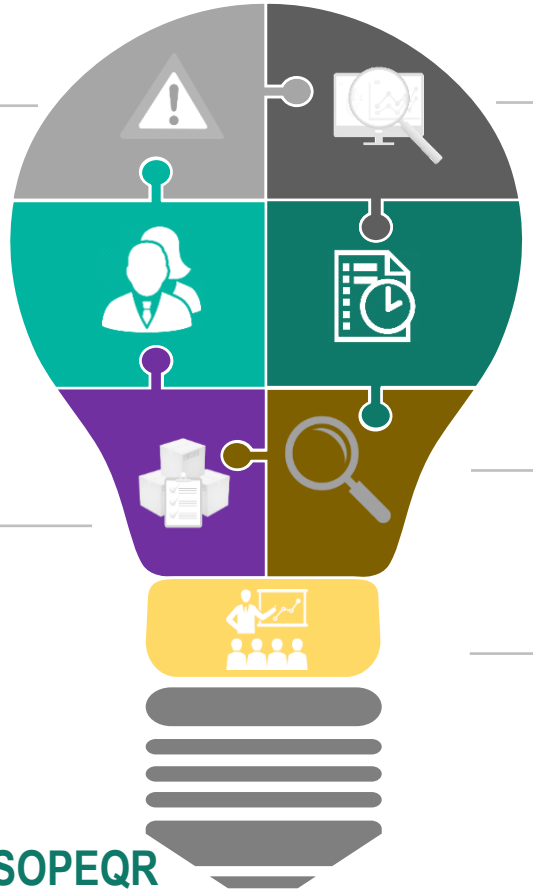
Tercero

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

Contenido del Documento de Seguridad

Artículo 37 de la LPDPPSOPEQR

Documento de seguridad



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

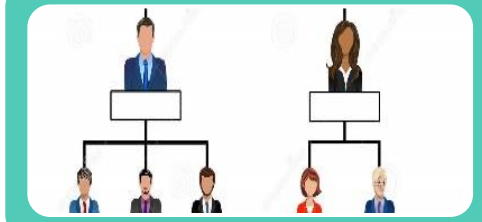
Artículo 4 fracción XV de la LPDPPSOPEQR

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

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

Obligaciones y prohibiciones en materia de seguridad de la información-seguridad de datos personales.

Precisiones de acuerdo a perfiles y privilegios que permitan asignar responsabilidades sobre el tratamiento de datos personales realizado.

PASO 3 – ELABORAR UN ANÁLISIS DE RIESGOS

Conocer las amenazas y vulnerabilidades que pueden afectar la seguridad de los datos personales que resguarda, y crear escenarios probables de materialización del riesgo, de acuerdo al valor de los activos.

PASO 4 – ELABORAR UN ANÁLISIS DE BRECHA

Identificar las medidas de seguridad físicas, técnicas y administrativas que están implementadas actualmente, las medidas de seguridad faltantes, y las que requiere implementar y mejorar en los sistemas de tratamiento

DOCUMENTO DE SEGURIDAD

PASO 5 – ELABORAR UN PLAN DE TRABAJO

Se deben puntualizar 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 garantizar que las medidas de seguridad implementadas protegen los datos personales de manera adecuada.

PASO 7 – DESARROLLAR UN PROGRAMA GENERAL DE CAPACITACIÓN

Plan para 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

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.

INVENTARIO DE DATOS PERSONALES

- Control documentado, sobre los tratamientos de datos personales realizados por las unidades administrativas de la Institución con orden y precisión, y está previsto en la LGPDPPSO (Art. 33 Frac III)

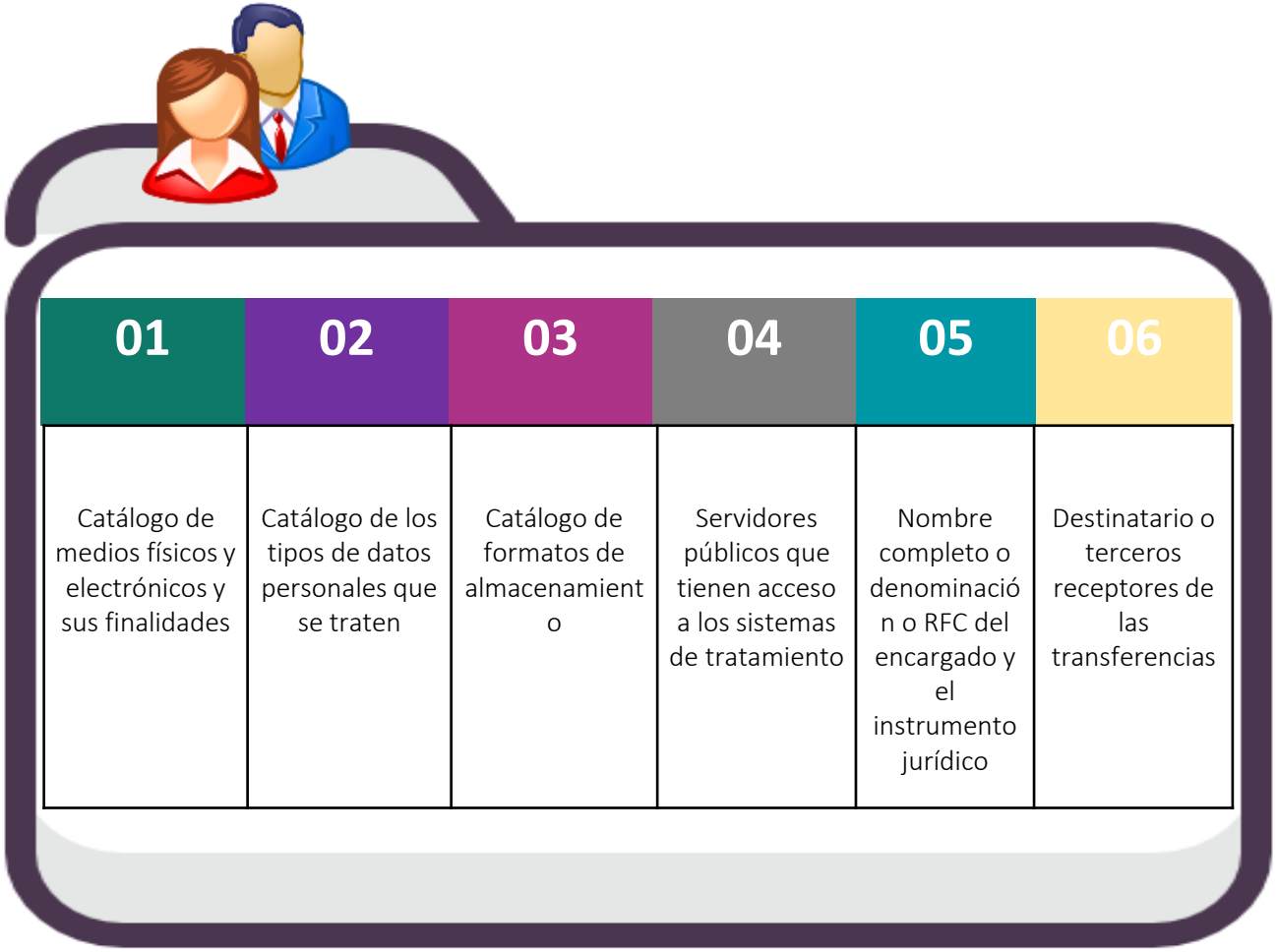
- Los elementos que debe incluir se definen en los Lineamientos Generales (Art. 58).

- 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



01	02	03	04	05	06
Catálogo de medios físicos y electrónicos y sus finalidades	Catálogo de los tipos de datos personales que se traten	Catálogo de formatos de almacenamiento	Servidores públicos que tienen acceso a los sistemas de tratamiento	Nombre completo o denominación o RFC del encargado y el instrumento jurídico	Destinatario o terceros receptores de las transferencias

INVENTARIO DE DATOS PERSONALES

¿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?

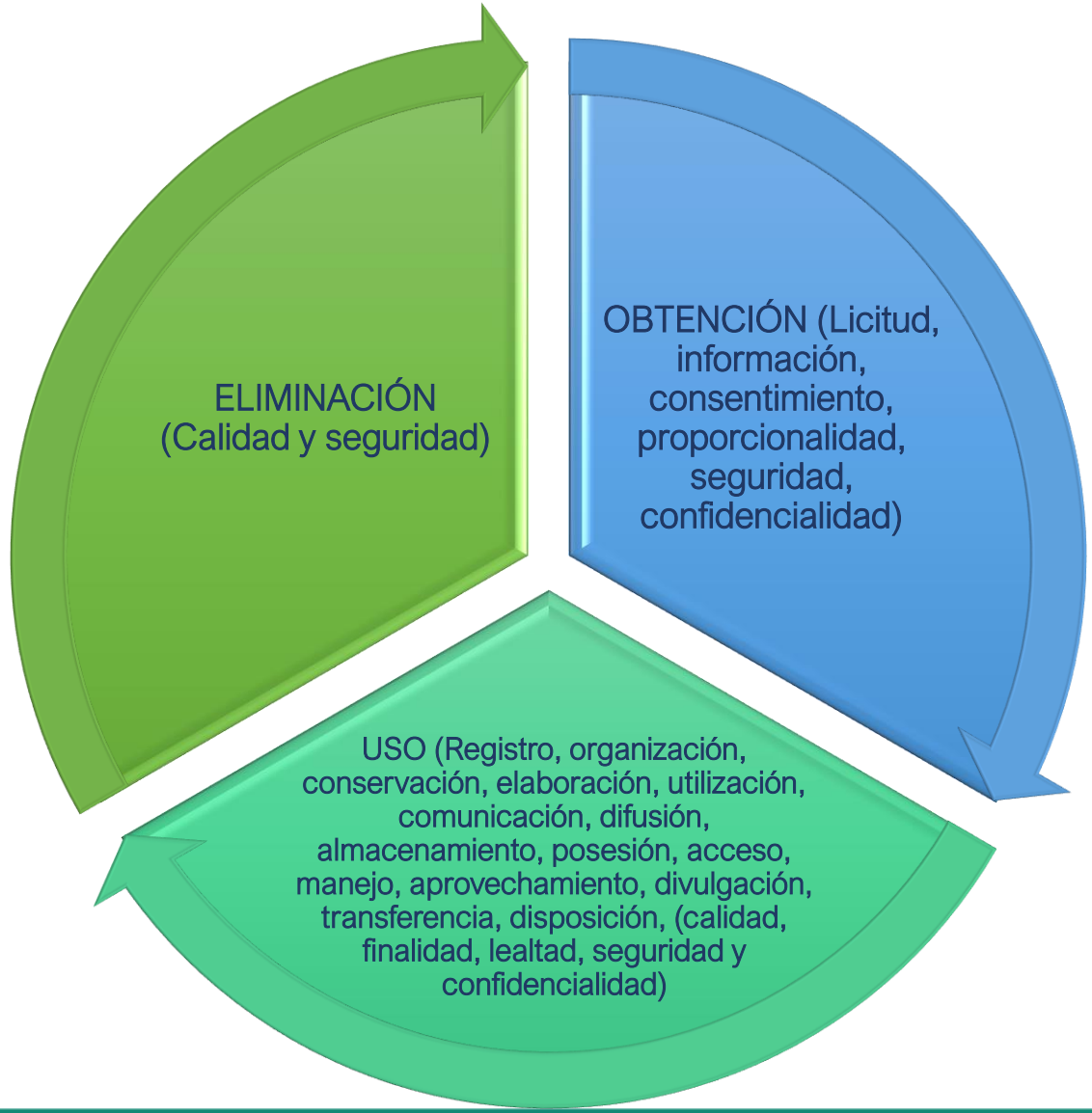
Diferentes personas pueden tener acceso a los sitios donde se almacenan los datos personales, estás pueden tener permisos específicos.

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.

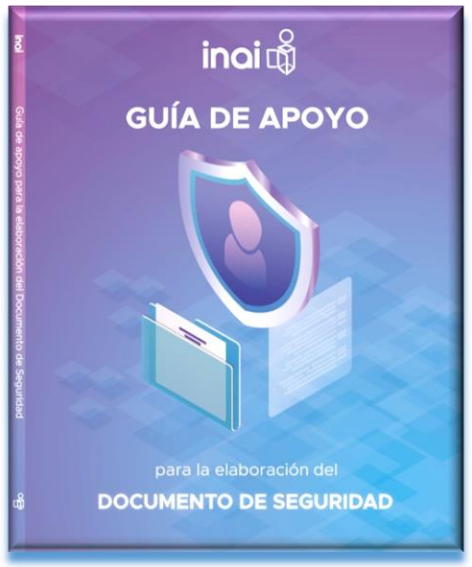
Y con ello posteriormente identificar el riesgo inherente de los datos personales. (art. 59 de los LGPDP).



INVENTARIO DE DATOS PERSONALES

- El INAI elaboró un Documento Orientador para la elaboración del Programa de Protección de Datos Personales, este se encuentra 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.



Definición del proceso

*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 Estat

- 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
- Terceros que transfieren los datos personales al INAI
- 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

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). Artículo 19 LPDPPSOPEQR

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.

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.

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

- 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

Art. 57 de los LGPDSP

ESTABLECER FUNCIONES Y OBLIGACIONES

Funciones y obligaciones de los que tratan datos personales

Definir **medidas de seguridad** para atender los riesgos identificados

- Establecer perfiles y privilegios adecuados
- Definir responsabilidades para la protección de los DP
- Establecer cadena de rendición de cuentas, en caso de vulneraciones de seguridad
- Identificar requerimientos específicos en materia de capacitación de DP

Conocer los **riesgos** asociados al tratamiento que realiza

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

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 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

sea parte de los valores

institucionales

a) **Comunicar** a los involucrados en el tratamiento de datos (internos y externos) la importancia de:

* **Cumplir** con la política de protección de datos personales.

** **Conocer los objetivos** del documento de seguridad, medidas de seguridad y sistema de gestión.

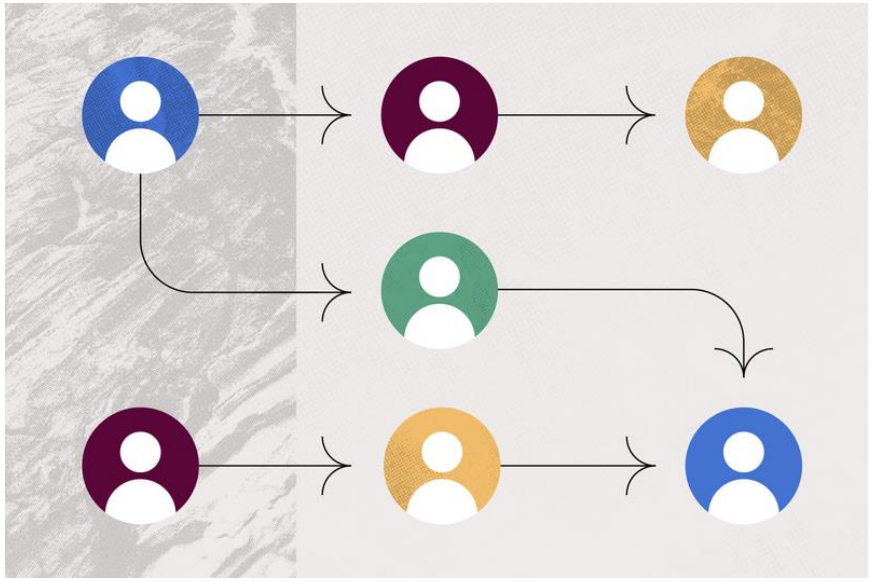
*** **Mejorar y actualizar** el documento de seguridad, medidas de seguridad y sistema de gestión.

b) **Definir los roles, responsabilidades**, cadena de rendición de cuentas y estructura organizacional,

c) **Asegurar que todos los integrantes del sujeto obligado tengan claro sus roles y funciones**, así como su contribución para el logro de objetivos de el documento de seguridad, medidas de seguridad y sistema de gestión y las consecuencias de su incumplimiento.

ESTABLECER FUNCIONES Y OBLIGACIONES DE QUIENES TRATEN DATOS PERSONALES

Cadena de rendición de cuentas



FUNCIONES	OBLIGACIONES	CAPACITACIÓN
Propietario del sistema	• Definidas por las actividades que realiza con el tratamiento de datos personales	• Definida por sus responsabilidades (básica, intermedia o especializada)
Administrador		• Especializada
Usuario genérico		• Definida por sus responsabilidades (básica, intermedia o especializada)
Custodio		• Especializada

ESTABLECER FUNCIONES Y OBLIGACIONES DE QUIENES TRATEN DATOS PERSONALES

FUNCIONES	PERFIL	DESCRIPCIÓN	OBLIGACIONES
Propietario del sistema	Titular de la Unidad Administrativa	Responsable del sistema de tratamiento	• Definir acciones para ejecutar el tratamiento de dato personales
Administrador	Personal designado por el propietario del sistema que puede tomar decisiones respecto al uso de la información	Responsable de asignar permisos a partir de las actividades que los usuarios realizaran	• Otorgar permisos y vigilar la ejecución de tareas asignadas
Usuario genérico	Personal que realiza actividades especificas a partir de los privilegios	Utilizador del sistema de tratamiento que interactua con la información del sistema de tratamiento (ver, modificar o eliminar información)	• Realizar sus actividades atendiendo las medidas de seguridad especificas para cuidar la Confidencialidad, Integridad y Disponibilidad de la Información
Custodio	Personal que tiene un encargo dentro del sistema sin tratar los datos que obran dentro del sistema de tratamiento	Personal que se encarga de la administración diaria de la seguridad en los sistemas de información y el monitoreo del cumplimiento de las políticas de seguridad en los sistemas que se encuentran bajo su administración	• Gestionar activos • Mantener las medidas de seguridad a los activos

3. ELABORAR UN ANÁLISIS DE RIESGOS

¿QUÉ ES UN RIESGO?

Riesgo. Es la posibilidad de sufrir pérdidas. 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.

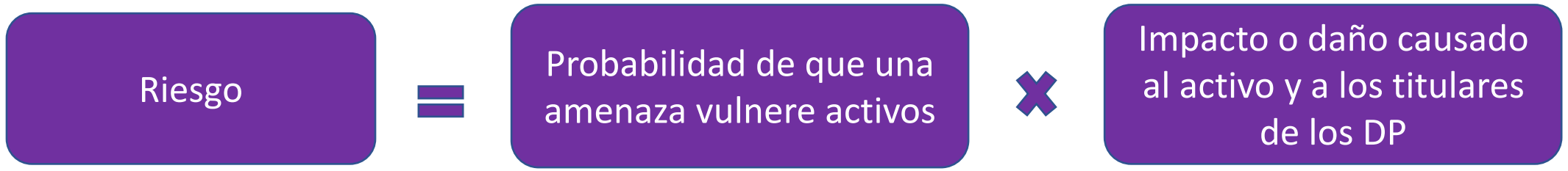
Amenaza: Circunstancia o condición externa, con la capacidad de causar daño a los activos (datos personales) explotando una o más de sus vulnerabilidades.

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

REALIZAR EL ANÁLISIS DE RIESGO DE LOS DATOS PERSONALES

Análisis de riesgo: Es el proceso para comprender la naturaleza del riesgo 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.



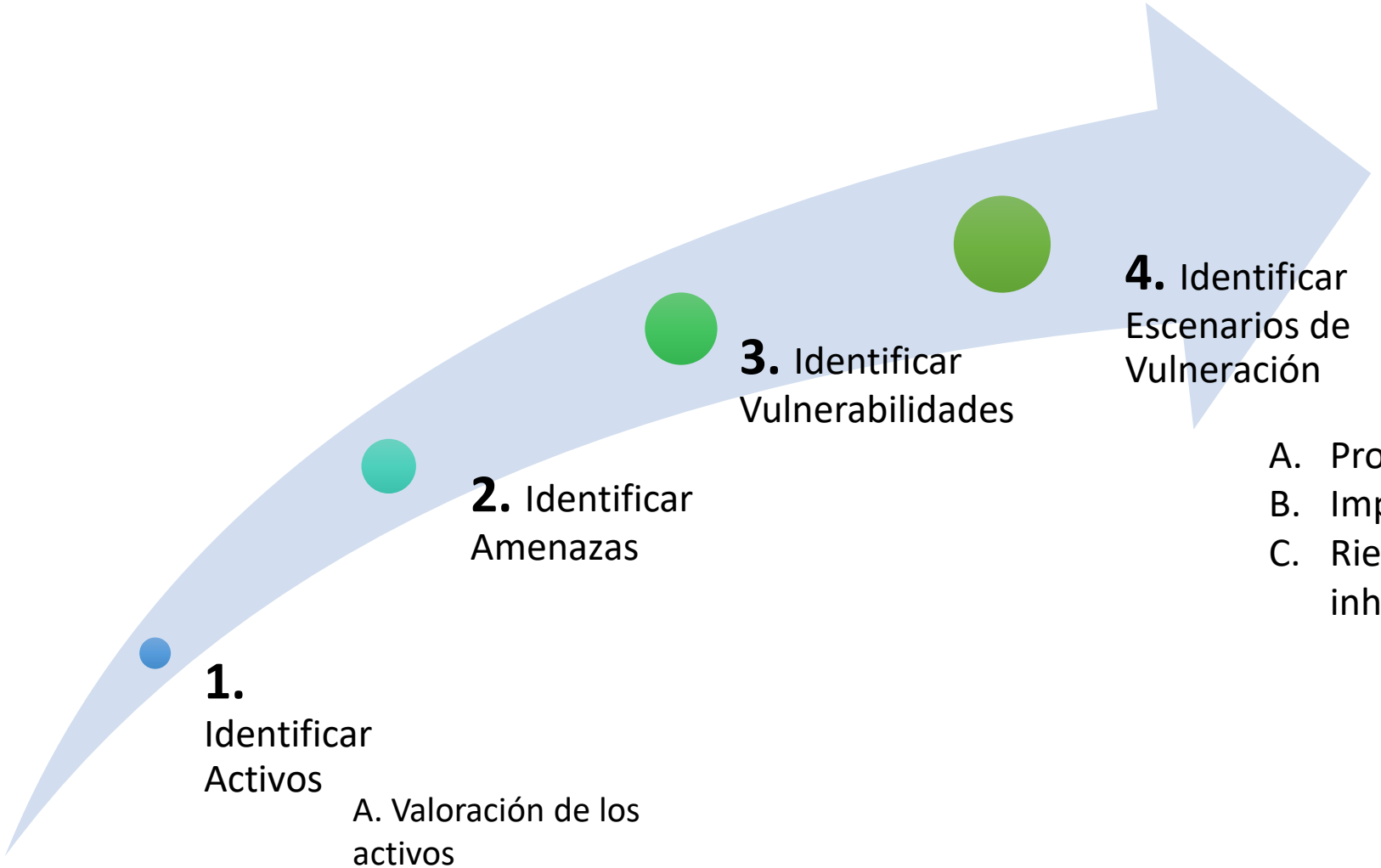
Los sujetos obligados deberán adoptar alguna metodología o a partir de alguna crear una propia para gestionar el riesgo.

Existen múltiples metodologías como:

- Serie ISO 27000 que contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Sistemas de Gestión de la Seguridad de la Información (SGSI), particularmente la ISO/IEC/27002 es código de buenas prácticas para la GSI, donde se mencionan los controles para las amenazas identificadas, y la ISO/IEC/27005 trata la gestión de riesgos en seguridad de la información.

- MAGERIT versión 3.0. una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados.

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

Gestión de riesgos. es el proceso continuo de identificación de riesgos y de implementación de acciones para abordarlos.

Se deben identificar, comprender, evaluar y mitigar los riesgos –y sus vulnerabilidades subyacentes– y el impacto en la información, los sistemas de información y las organizaciones que dependen de la información para sus operaciones.

No existe la seguridad total. 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 identificar los riesgos, amenazas, vulnerabilidades e involucrados, documentarlos y determinar la tolerancia del responsable, estableciendo las opciones de gestión que se aplicará a cada riesgo.

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

DEFINICIÓN DE LA VALORACIÓN DE LOS DATOS

Una vez identificados los elementos a analizar para evaluar los riesgos, es necesario definir una escala de medición para los siguientes elementos:

- Valor de riesgo
- Probabilidad de ocurrencia
- Impacto

Escalas

- Los datos cualitativos se expresan en forma de palabras o textos que ayudan a comprender ciertas acciones que no son cuantificables
- Los datos cuantitativos consisten en cualquier información cuantificable que pueda utilizarse para realizar cálculos matemáticos y análisis estadísticos
- Los datos combinados se refieren a una combinación entre la cuantitativa y la cualitativa

NIVEL DE RIESGO	ACCIÓN REQUERIDA
ALTO	Inaceptable: acciones deben tomarse inmediatamente
MEDIO	Razonablemente aceptable: acciones requeridas y que deben tomarse en plazo razonable
BAJO	Aceptable: no se requieren acciones de inmediato

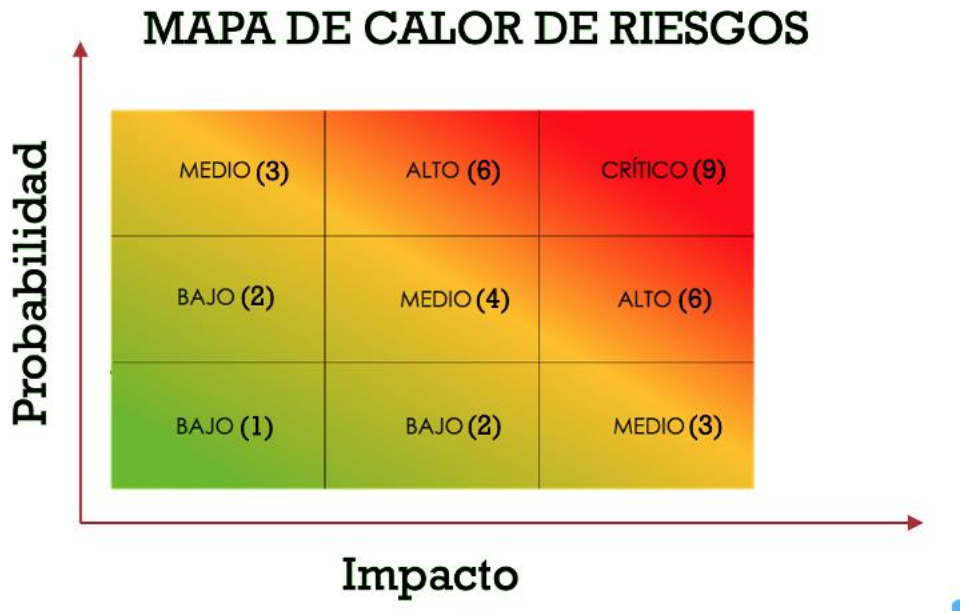
Probabilidad	Importancia	Frecuencia	Impacto
Poco probable	Baja	Poco frecuente	Bajo
Probable	Media	Regularmente	Medio
Bastante probable	Alta	Frecuentemente	Alto

Números fijos	Escalas	Rangos
1	1/10	1-3
2	5/10	4-6
3	10/10	7-9

Combinación 1
1 – bajo
2 – moderado
3 - serio

DEFINICIÓN DE LA MÉTRICA PARA GESTIONAR EL RIESGO

Impacto		Probabilidad		Nivel de riesgo	
Cuantitativo	Cualitativo	Cuantitativo	Cualitativo	Cuantitativo	Cualitativo
1	Bajo	1	Bajo	1	Bajo
1	Bajo	2	Medio	2	Bajo
2	Medio	1	Bajo	2	Bajo
1	Bajo	3	Alto	3	Medio
3	Alto	1	Bajo	3	Medio
2	Medio	2	Medio	4	Medio
2	Medio	3	Alto	6	Alto
3	Alto	2	Medio	6	Alto
3	Alto	3	Alto	9	Critico

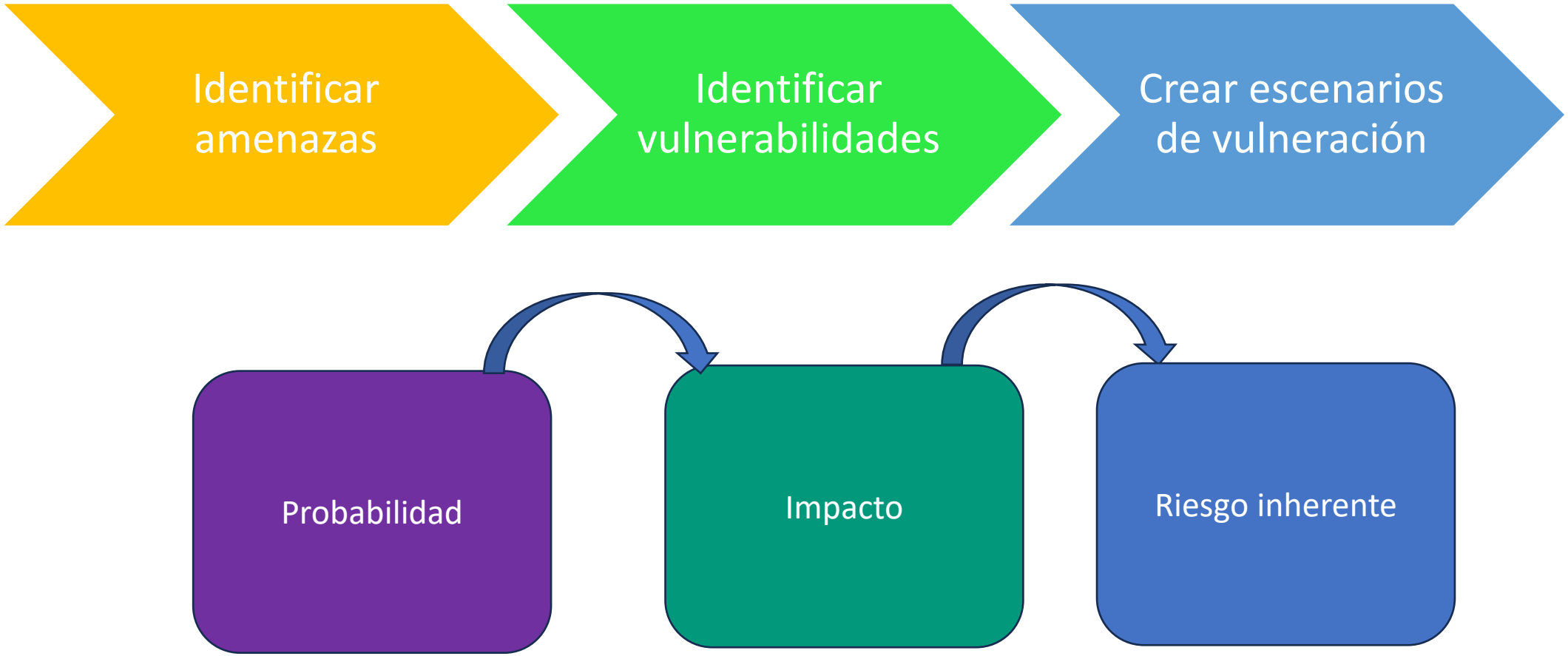


Identificar y valorar activos

1. Identificar activos

2. Valorar activos

Por cada activo:



- Criterios de Probabilidad

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:

En este paso se debe asignar un valor a la posibilidad de que un evento ocurra, en dos dimensiones, cuando se tienen registros (valor de frecuencia) y cuando no se tienen registros (valor de factibilidad).

- Probabilidad por frecuencia

Es la valoración más recomendable ya que incluye una evidencia que sustenta el calculo realizado.

- Probabilidad por factibilidad:

Es la evaluación de la magnitud de las consecuencias de un evento, si ocurriera, y la posibilidad del evento y sus consecuencias asociadas, como alternativa, cuando no hay a disposición datos del pasado, se pueden hacer estimaciones subjetivas que reflejen el grado de creencia de un individuo o grupo con respecto a la probabilidad de ocurrencia de un evento o resultado particular.

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 propiedades de seguridad de la información (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.

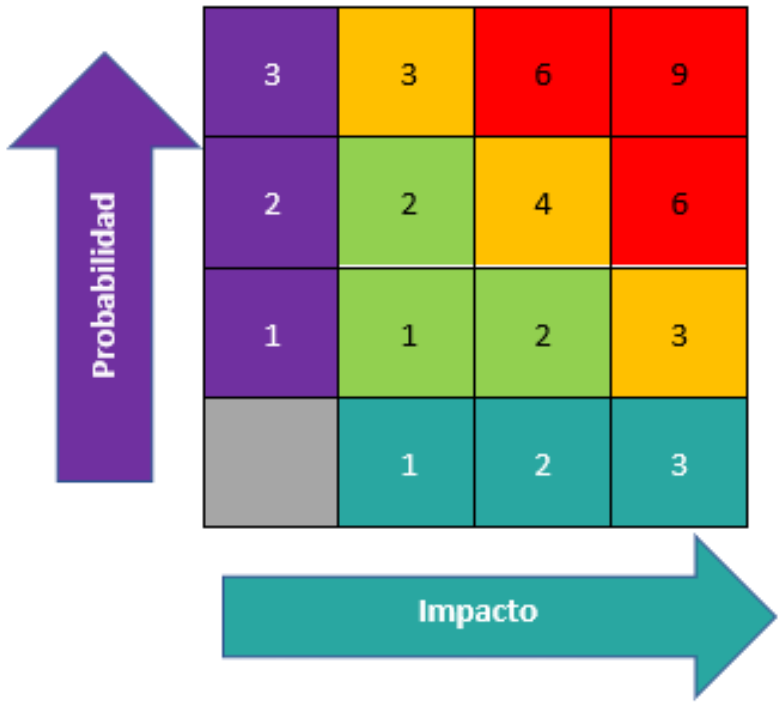
$$\text{impacto total} = \frac{\text{confidencialidad} + \text{integridad} + \text{disponibilidad}}{3}$$

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.

Valoración del riesgo inherente

Riesgo= probabilidad x impacto

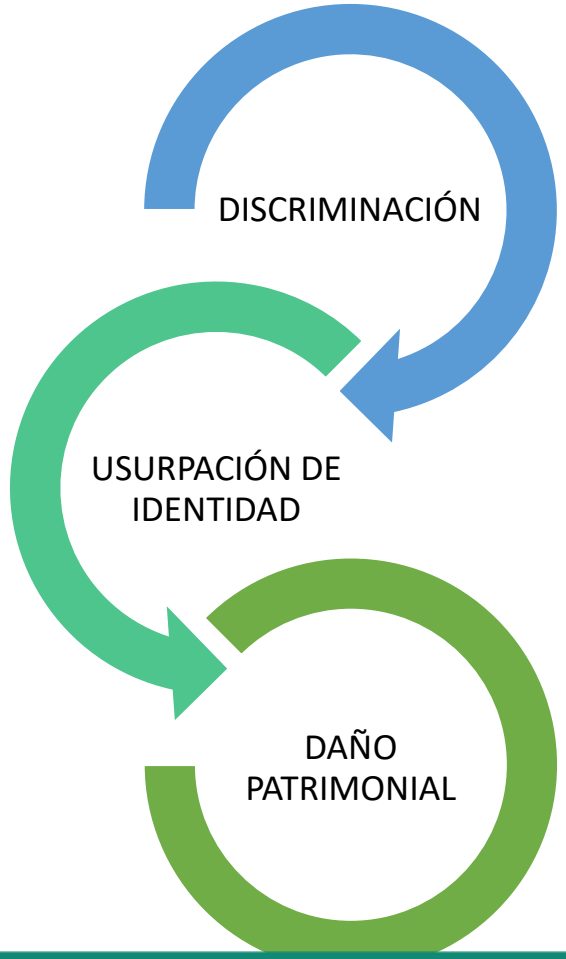
Teniendo valores cualitativos y cuantitativos podemos valorar el riesgo, para ello podemos utilizar una matriz de riesgo o un mapa de calor, como el siguiente ejemplo:



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.

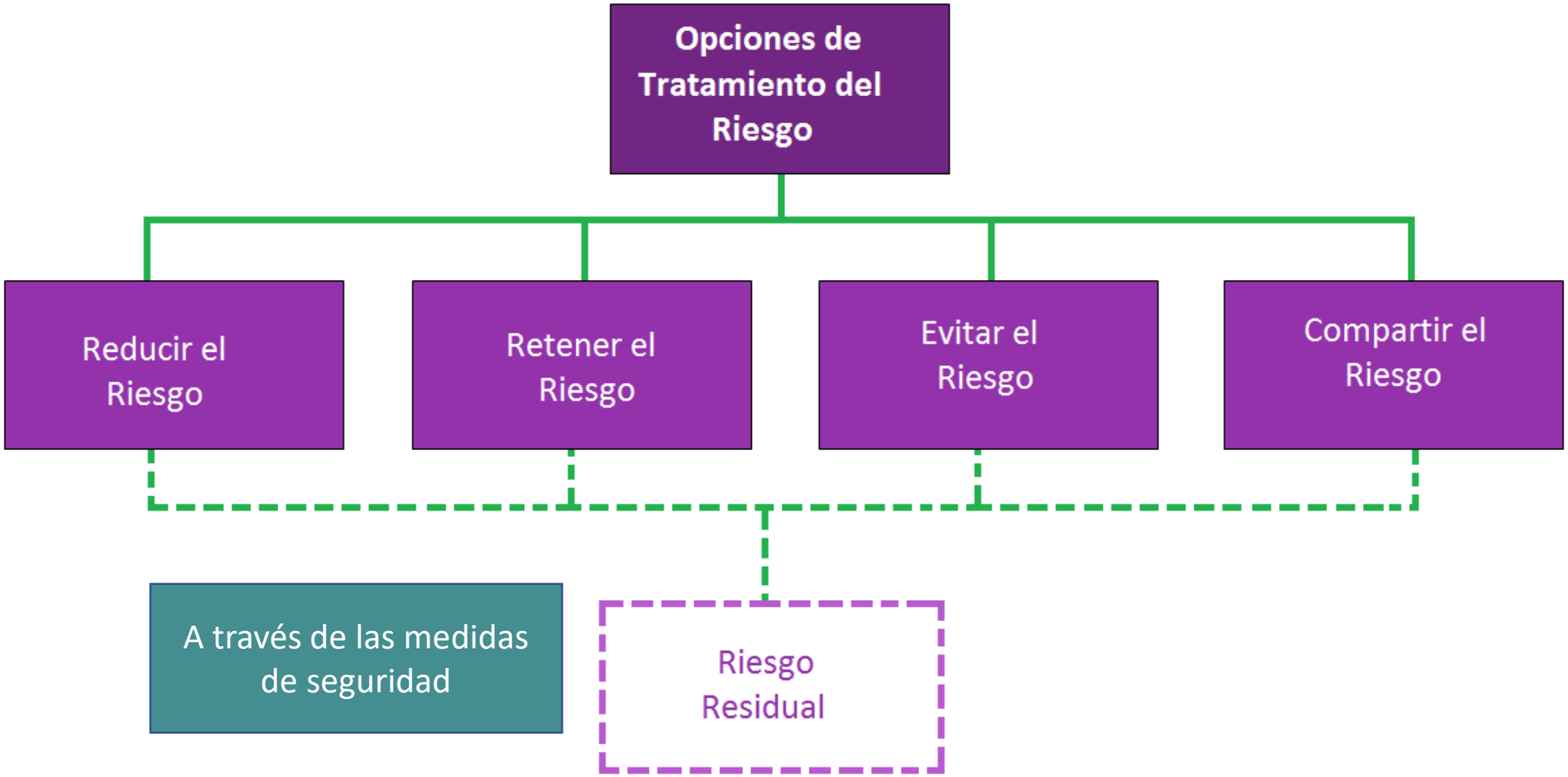


IDENTIFICACIÓN DEL RIESGO				ANÁLISIS DE RIESGO					EVALUACIÓN DE RIESGO
NOMBRE DEL ACTIVO	TIPO DE ACTIVO	VULNERABILIDAD	AMENAZA	PROBABILIDAD	Confidencialidad	Integridad	Disponibilidad	IMPACTO	RIESGO INHERENTE
Escriba el nombre del activo	Describa el tipo de activo a valorar	Describa la vulnerabilidad del activo	Describa la amenaza a la que se enfrenta	Seleccione un valor	Seleccione un valor	Seleccione un valor	Seleccione un valor	Realice el promedio de las columnas Confidencialidad, Integridad y Disponibilidad	Multiplique los valores asignados en impacto y probabilidad

Artículo 40. Además de las que señalen las leyes respectivas y la normatividad aplicable, se consideran como vulnerables de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:
I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada

4. ELABORAR UN ANÁLISIS DE BRECHA

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.

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 remplazar 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 34 fracción V de la Ley Local 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 33 de la Ley local 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.

DEFINICIÓN DEL ANÁLISIS DE BRECHA

Al conocer el objetivo del análisis de brecha y su relación con el análisis de riesgos, viendo al análisis de brecha como 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 del riesgo identificado, por lo que, podemos describir tres actividades que integra el análisis de brecha:

- La primera, 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.
- La segunda, se refiere a una valoración que describa la eficacia del control implementado al asociar la medida con la modificación del nivel de riesgo.
- Finalmente, determinar a partir de la descripción de la o las medidas de seguridad observadas el nivel de madurez que se tiene.

ANÁLISIS DE BRECHA

En esta etapa se busca identifcar las brechas de seguridad que quedaron evidenciadas en el analisis de riesgos, para que a partir de la defnición del tratamiento de riesgo que se realizara, se pueden tomar acciones para cerrarlas.

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

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.

Valoración de la medida

- En esta etapa 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 analisis de riesgos pero ahora con nuevos elementos que permiten determinar la disminución del riesgo en probabilidad o impacto.

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.

EVALUACIÓN DE RIESGO	ANALISIS DE BRECHA										
RIESGO INHERENTE	¿Tiene medidas de seguridad?	CATEGORÍA	OBJETIVO DE CONTROL	DESCRIPCIÓN DE LA O LAS MEDIDAS DE SEGURIDAD	NIVEL DE MADUREZ	NUEVA PROBABILIDAD	Nueva Confidencialidad	Nueva Integridad	Nueva Disponibilidad	NUEVO IMPACTO	RIESGO RESIDUAL
Resultado	Responda la pregunta	Identifique la categoría de seguridad que quiere desplegar	Describa el objetivo del control de seguridad	Describa la medida de seguridad	Identifique el nivel de madurez de la medida de seguridad de las opciones a desplegar	Seleccione el valor de probabilidad con la flecha de selección	Seleccione el valor de Confidencialidad con la flecha de selección	Seleccione el valor de Integridad con la flecha de selección	Seleccione el valor de Disponibilidad con la flecha de selección	Resultado	Resultado

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

Cumplir con la política 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:

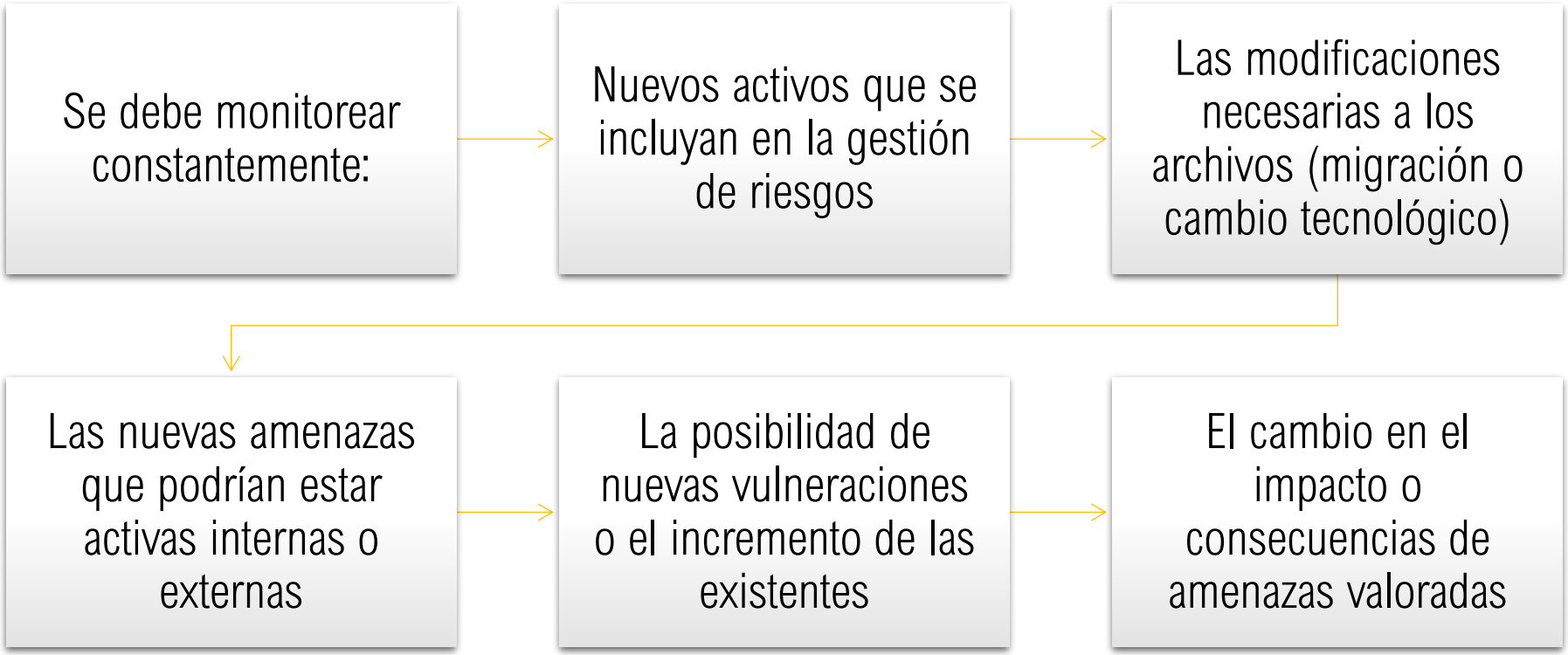
1.
   - Defina acciones a implementar.
   - La selección de las acciones prioritarias.
2.
   - Ser acorde al resultado del análisis de riesgo y análisis de brecha.
   - El periodo en el que se pretende cumplir esas acciones.
3.
   - Priorizar las medidas de seguridad más relevantes e inmediatas a establecer de acuerdo al nivel de riesgo.
   - Los recursos humanos y materiales para el cumplimiento de las acciones.

PLAN DE TRABAJO						
ACTIVIDAD A REALIZAR	TIEMPO ESTIMADO PARA SU EJECUCIÓN	FECHA DE INICIO	ENCARGADO DE EJECUCIÓN	VALIDADOR DE IMPLEMENTACION	PRESUPUESTO ESTIMADO	COMENTARIOS ADICIONALES
Escriba la actividad a realizar	Indique el tiempo estimado para la ejecución de la medida de seguridad	Indique la fecha de inicio	Nombre al encargado de la ejecución de la Medida de seguridad	Nombre al validador de la ejecución de la Medida de seguridad	Indique el presupuesto estimado para la ejecución	Describa si tiene un comentario adicional

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

MONITOREO Y SUPERVISIÓN
art. 63 lineamientos generales

El sujeto obligado deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales:



Revisión de los factores de riesgo

Auditoría

Vulneraciones a la Seguridad de la Información

Revisiones de factores de riesgo

Tipo de medida de seguridad	Descripción de la medida de seguridad	Monitoreo	Tiempo para la revisión	Resultado del monitoreo
Físicas				
Administrativas				
Técnicas				

MONITOREO Y SUPERVISIÓN
ART. 63 LINEAMIENTOS GENERALES

Auditoría

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

Artículo 155. Los Responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable.

AUDITORÍA VOLUNTARIA

Solicita	Realiza	Objeto
Responsables	INAI	Constatar adaptación, adecuación y eficacia
Voluntariamente	Organismos garantes	controles, medidas y mecanismos implementados
		para cumplimiento de Ley y demás normativa

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.

Programa General de Capacitación

- Sensibilización a personal interno y externo
- Capacitación básica a personal interno y externo
- Capacitación especializada – de acuerdo a roles y responsabilidades
- Cultura organizacional en seguridad de la información y protección de datos personales

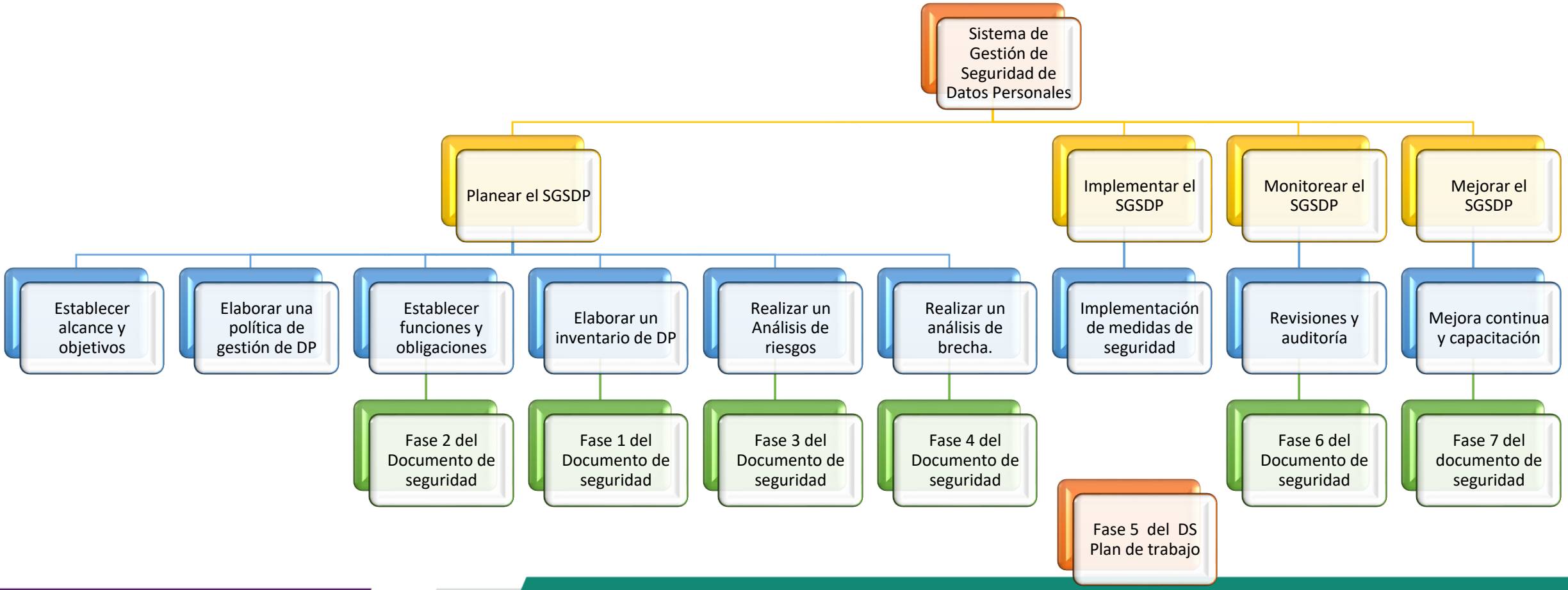
Documento de seguridad

¿CUÁNDO SE ACTUALIZA?

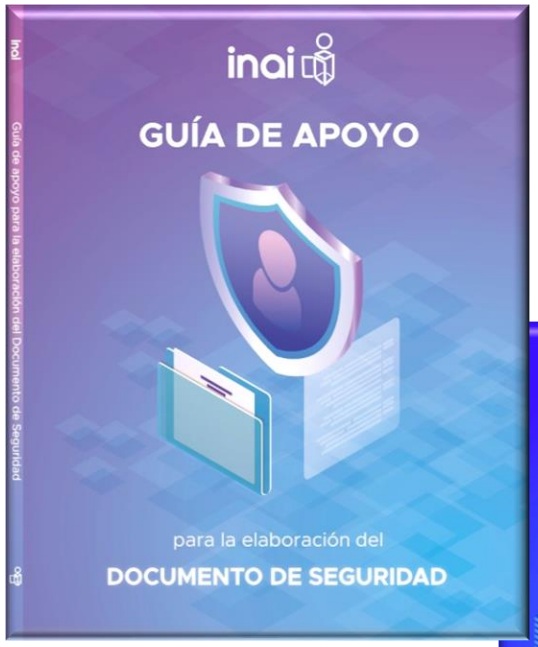
Cuando ocurran los siguientes eventos (Artículo 36 LGPDPPSO):

- 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.

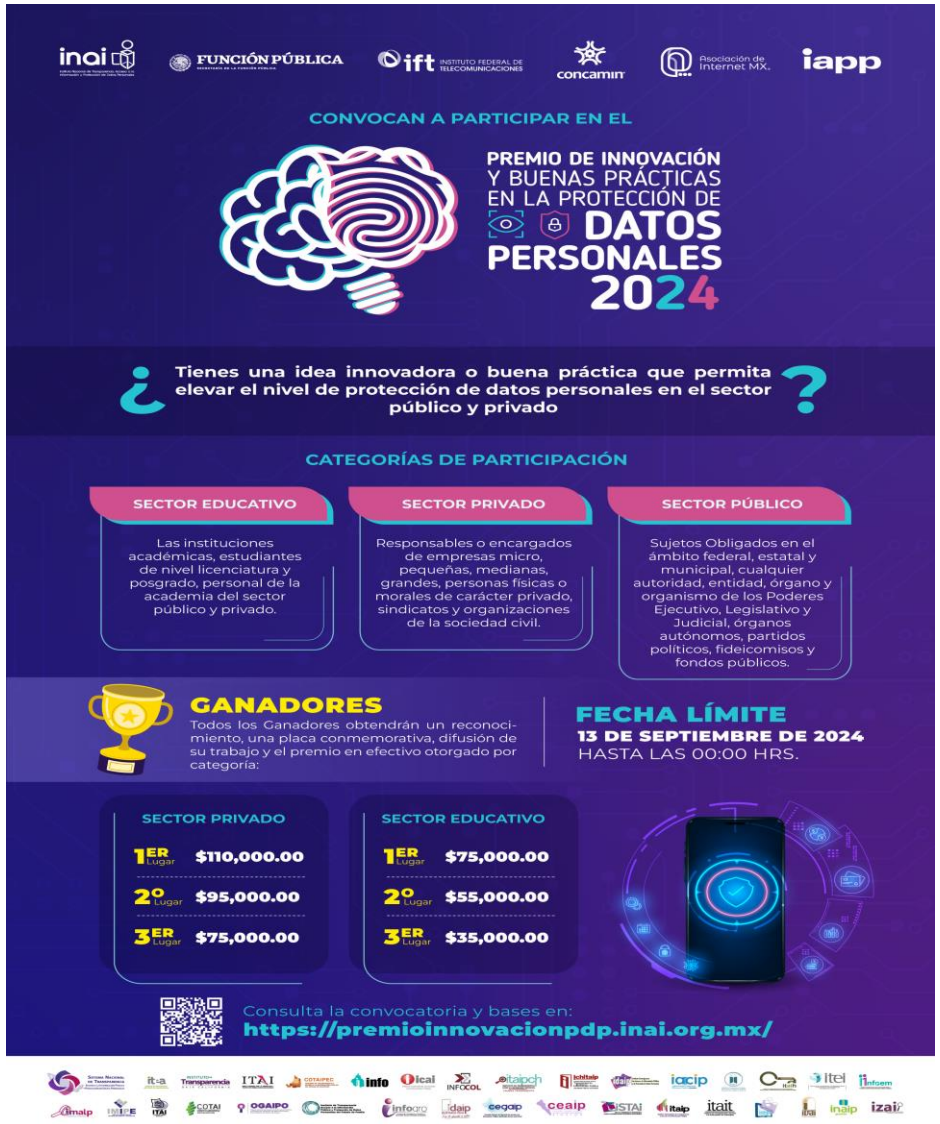
EL DOCUMENTO DE SEGURIDAD Y EL SISTEMA DE GESTIÓN DE DATOS PERSONALES



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



inai
Conoce la
GUÍA DE APOYO PARA LA ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD
que el INAI tiene para ti
inai
GUÍA DE APOYO
para la elaboración del
DOCUMENTO DE SEGURIDAD
DESCARGA EL PDF
Síguenos en
INAI México


CONVOCAN A PARTICIPAR EN EL
PREMIO DE INNOVACIÓN Y BUENAS PRÁCTICAS EN LA PROTECCIÓN DE DATOS PERSONALES 2024
¿Tienes una idea innovadora o buena práctica que permita elevar el nivel de protección de datos personales en el sector público y privado?
CATEGORÍAS DE PARTICIPACIÓN
SECTOR EDUCATIVO
Las instituciones académicas, estudiantes de nivel licenciatura y posgrado, personal de la academia del sector público y privado.
SECTOR PRIVADO
Responsables o encargados de empresas micro, pequeñas, medianas, grandes, personas físicas o morales de carácter privado, sindicatos y organizaciones de la sociedad civil.
SECTOR PÚBLICO
Sujetos Obligados en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.
GANADORES
Todos los Ganadores obtendrán un reconocimiento, una placa conmemorativa, difusión de su trabajo y el premio en efectivo otorgado por categoría:
FECHA LÍMITE
13 DE SEPTIEMBRE DE 2024
HASTA LAS 00:00 HRS.
SECTOR PRIVADO
1ER Lugar $110,000.00
2º Lugar $95,000.00
3ER Lugar $75,000.00
SECTOR EDUCATIVO
1ER Lugar $75,000.00
2º Lugar $55,000.00
3ER Lugar $35,000.00
Consulta la convocatoria y bases en:
https://premioinnovacionpdp.inai.org.mx/

CONVOCAN AL
CONCURSO
PARA SER COMISIONADA Y COMISIONADO INFANTIL
y formar parte del Pleno Niñas y Niños 2024
Realiza un video de máximo 3 minutos en donde expongas cómo proteger tus datos personales
¡Escanea y consulta la convocatoria!
Síguenos en INAI México
Si tienes de 10 a 12 años cumplidos. ¡Participa!
Conoce los videos ganadores del 2023
Fecha límite: 28 de junio de 2024 • 23:59 horas
¿Si tienes dudas? (55) 50042400, ext. 2529, 2558 y 2326

GRACIAS

DIRECCIÓN GENERAL DE PREVENCIÓN Y AUTORREGULACIÓN

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

Lic. Katherine Esparza Cortéz
Directora de Seguridad de Datos Personales del Sector Público
Correo electrónico: katherine.esparza@inai.org.mx

Lic. Damian Vicente Guerrero
Subdirector de Seguridad de Datos Personales del Sector Público
Correo electrónico: damian.vicente@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