IMIPE

INSTITUTO MORELENSE DE
INFORMACIÓN PÚBLICA Y ESTADÍSTICA

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

Temario

Tema 6 Sistemas de Gestión

6.1 Recursos de la Organización

6.2 Planteamiento del modelo de seguridad
- 6.2.1 Gestión de riesgos
- 6.2.2 Ciclo Deming
- 6.2.3 Wh Questions

6.3 Sistemas de Gestión
- 6.3.1 Sistemas de gestión
- 6.3.2 Sistemas de Gestión de Seguridad de la Información (SGSI)
- 6.3.3 Sistemas de Gestión de Seguridad de Datos Personales (SGSDP)

6.4 ISO 27001
- 6.4.1 Generalidades
- 6.4.2 Indicadores de gestión
- 6.4.3 Esquema de implantación de un SGSI

6.5 Recomendaciones de implantación del SGSDP
- 6.5.1 Contexto organizacional
- 6.5.2 Identificación de interesados
- 6.5.3 Identificación de Requerimientos
- 6.5.4 Planificación de la implantación
- 6.5.5 Evaluación y monitoreo
- 6.5.6 Mejora continua

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

Tema 6 Sistemas de Gestión

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.1 Recursos de la Organización

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

ORGANIZACIÓN

↓

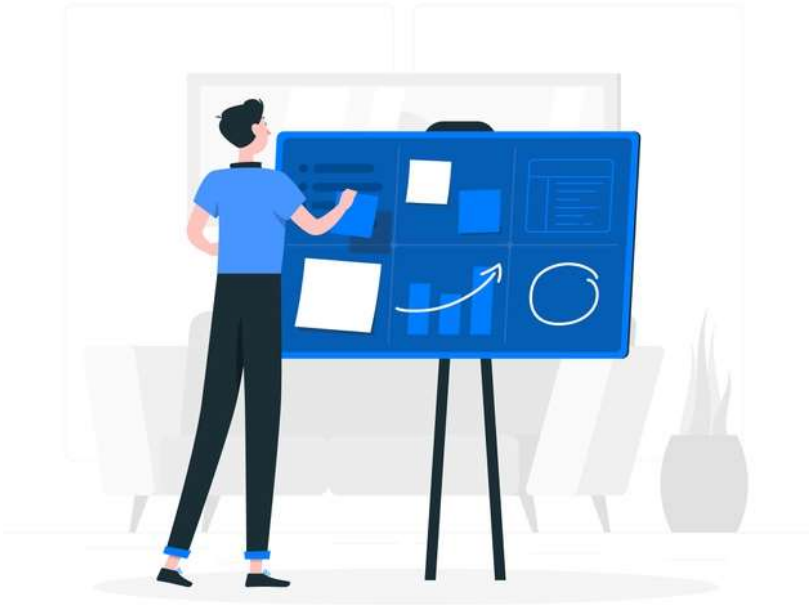
ACTIVOS (Recursos)

R.H | R.M. | R.F.

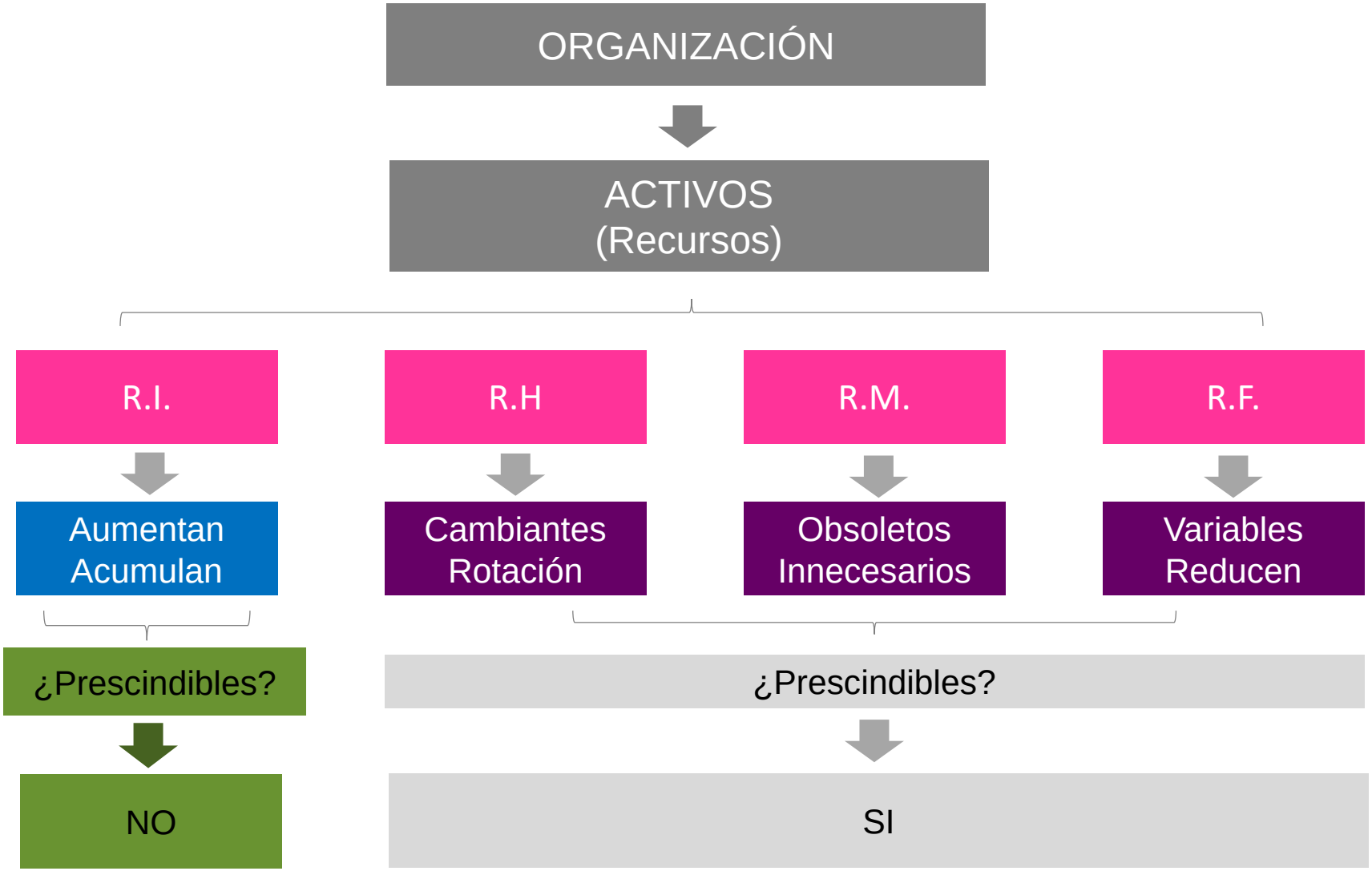
PRODUCTOS / SERVICIOS
(El trabajo que permite alcanzar los objetivos)

DOCUMENTOS | CONOCIMIENTO

INFORMACIÓN



SGS DP
SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES



Activos de Información

Las bases de datos y los archivos, constituyen los recursos de información de las organizaciones y conforman la Base de Conocimiento (Knowledge Base).

Los activos de información son los únicos que, en una organización debidamente funcional, se incrementan de forma permanente y, en la actualidad, de manera exponencial

El valor que la información y el conocimiento tienen para la organización, genera “apetito” entre aquellos que buscan amenazarla.

Las amenazas se diversifican y aumentan cada día.

Garantizar la seguridad de los activos de información es fundamental e indispensable, pero debe hacerse de manera correcta, sistemática y documentadamente, es por ello que se requiere plantear un modelo de seguridad para la organización.

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.2 Planteamiento del Modelo de Seguridad

Considerando que los activos de información deben ser asegurados por las organizaciones, se debe plantear el modelo de seguridad que se utilizará para protegerlos.

Cualquier modelo que se determine, debe considerar:

- Identificación de riesgos
- Identificación de amenazas
- Identificación de vulnerabilidades
- Identificación de interesados
- Evaluación del impacto / daño
- Establecimiento de planes de acción

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.2.1 Gestión de riesgos (Risk Management)

Riesgo: Acontecimiento que afectaría negativamente a la organización, en caso de ocurrir.

Amenaza: Potencial ocurrencia de un riesgo (materialización del riesgo).

Vulnerabilidad: Debilidad o deficiencias de seguridad en una organización o sistema (aprovechado por el factor amenazante).

Impacto: Afectación que ocurre si se materializa la amenaza

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.2.1 Gestión de riesgos (Risk Management)

No existe la seguridad total: Los riesgos y amenazas siempre existen, sin importar la cantidad de recursos que destine la alta dirección para su atención, por ello se debe realizar una gestión de riesgos acorde a los objetivos y capacidades de la organización.

La gestión de riesgos considera identificar los riesgos, amenazas, vulnerabilidades e involucrados (stakeholders), documentarlos y determinar la tolerancia de la organización, 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.

SGS DP
SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.2.1 Gestión de riesgos (Risk Management)

Los riesgos pueden ser:

- Prevenidos
- Transferidos
- Minimizados o mitigados
- Asumidos o aceptados

PLANES DE ACCIÓN

- Sistemáticos
- Estructurados
- Repetibles
- Eficientes
- Adaptables

Como resultado:

Riesgos secundarios

Riesgos residuales

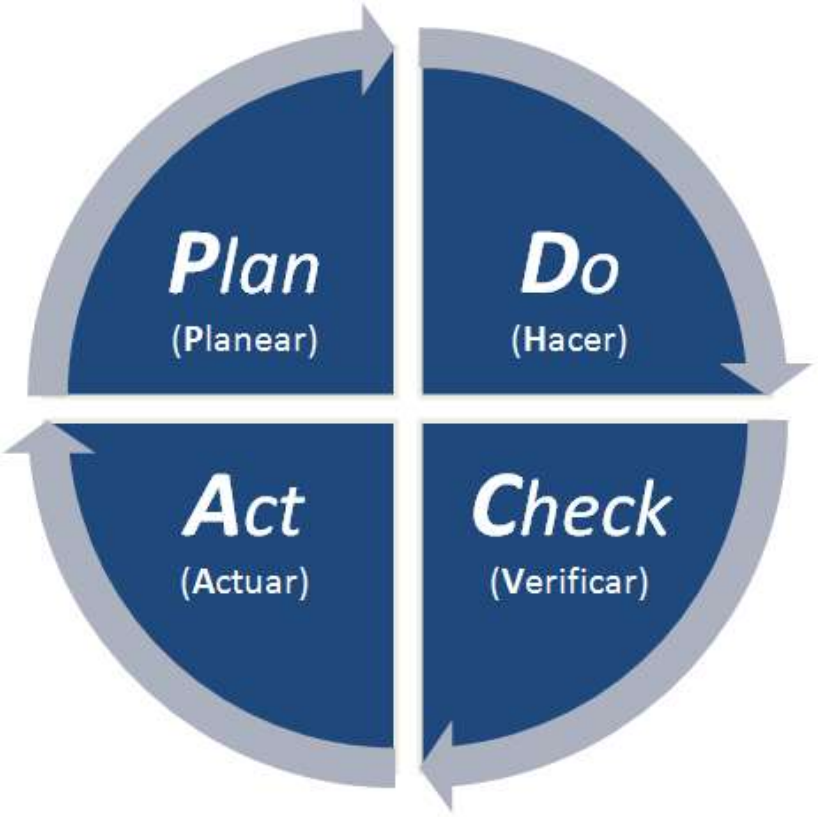
La gestión de riesgos debe considerar a todos los involucrados (stakeholders), ya sean aquellos que resultan en factores amenazantes, los que deben actuar conforme al plan de acción, y a los que recibirán un impacto tras la implementación del plan.

Los stakeholders siempre pueden ser internos o externos y este aspecto debe considerarse en el plan de acción.

SGS DP

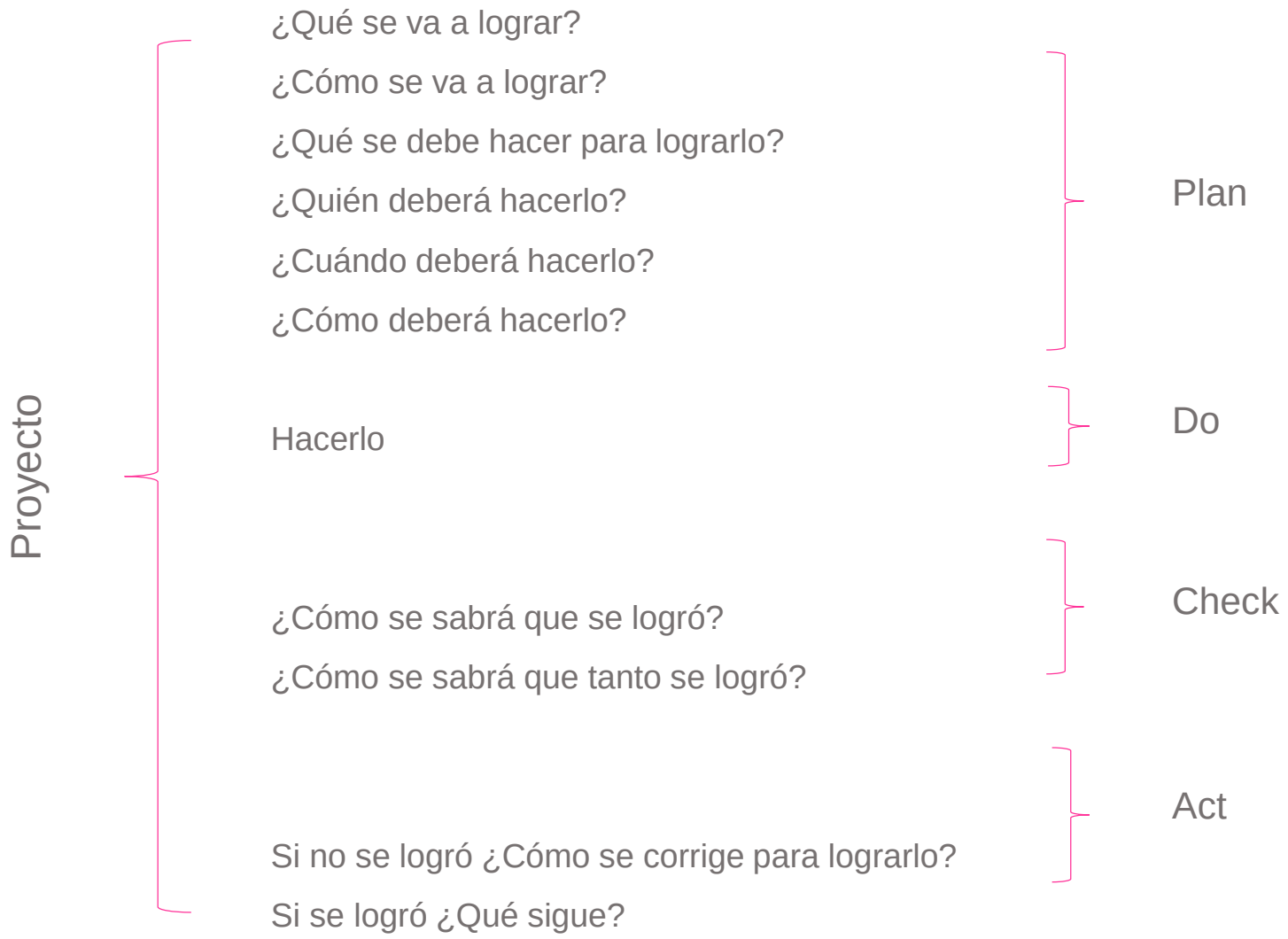
SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.2.2 Ciclo Deming



SGS DP
SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.2.2 Ciclo Deming



SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.2.3 WH Questions

Las WH Questions se denominan así porque se refieren a preguntas que tienen esas letras en común.

Estas son las preguntas que usualmente se deben hacer cuando emprendemos un trabajo o un proyecto.

What? - ¿Qué se tiene que proteger?	➡ Los activos de información
When? - ¿Cuándo se debe proteger?	➡ Mientras está en mi poder (tratamiento)
Where? - ¿Dónde se protege?	➡ Donde lo tenga (soporte)
Who? - ¿Quién lo protege?	➡ El responsable
Which? - ¿Cuáles se protegen?	➡ Los datos personales (contexto)
Why? - ¿Porqué se debe proteger?	➡ Obligaciones normativas
How? - ¿Cómo se protege?	➡ Sistemas de Gestión

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.3 Sistemas de Gestión

Un Sistema de Gestión se alinea a los objetivos institucionales y busca su logro, asegurando la mejora permanente de sus procesos y, por ende, de la organización.

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.3.1 Sistemas de Gestión

Según la RAE, un sistema es “un conjunto de cosas que, relacionadas entre sí ordenadamente, contribuyen a determinado objeto”.

Entonces, un sistema de gestión se trataría de “un conjunto de cosas que, relacionadas entre sí ordenadamente, contribuyen a gestionar y administrar una organización”.

Según ISO 9000, un sistema de gestión es “un sistema para establecer la política y los objetivos y para lograr dichos objetivos”.

Según la European Foundation for Quality Management, un sistema de gestión es “un esquema general de procesos y procedimientos que se emplea para garantizar que la organización realiza todas las tareas necesarias para alcanzar sus objetivos”

Los sistemas de gestión tienen su base en el ciclo de mejora continua (Ciclo Deming), con el objetivo de verificar el cumplimiento de metas y la correspondiente modificación o corrección de los procesos de la organización basados en los resultados obtenidos.

Dicho de otro modo, **un sistema de gestión busca establecer y garantizar el logro de los objetivos y mantener en un proceso de mejora permanente a la organización.**

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.3.2 Sistemas de Gestión de Seguridad de la Información

Un sistema de gestión de seguridad de la información (SGSI), proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información para lograr los objetivos de negocio.

El análisis de los requisitos para la protección de los activos de información y la aplicación de controles adecuados para garantizar la protección de estos activos de información, contribuye a la exitosa implementación de un SGSI.

El SGSI ayuda a la organización a establecer las políticas, procedimientos y controles en relación a los objetivos de negocio de la organización.

6.3.3 Sistemas de Gestión de Seguridad de Datos Personales

Un sistema de gestión de seguridad de datos personales (SGSDP), busca garantizar la seguridad de los datos personales, en este caso, que se encuentran en posesión de los sujetos obligados, mediante la identificación de los procesos por medio de los cuales se obtienen dichos datos, su tratamiento y conservación, así como las medidas implementadas por el Sujeto Obligado para su adecuado resguardo.

El SGSDP debe estar alineado a los objetivos del Sujeto Obligado, considerando la normatividad que lo rige y el contexto propio de la institución.

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.4 ISO 27001

“Sistemático, documentado y conocido por toda la organización”

Un SGSI ayuda a la organización a establecer las políticas, procedimientos y controles en relación a los objetivos de negocio de la organización.

ISO 27001 se construye sobre el concepto central del SGSI

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.4.1 Generalidades

ISO 27001 es un estándar internacional para gestionar la seguridad de la información, cubriendo áreas de las cuales depende la seguridad de la organización.

Considera la seguridad técnica, de procesos, de personas y sus relaciones y de políticas.

ISO 27001 es un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información, el análisis de los requisitos para protegerlos y la aplicación de controles adecuados.

La seguridad de la información, según ISO 27001, consiste en la preservación de su **Confidencialidad, Integridad y Disponibilidad.**

De acuerdo a lo establecido en ISO 27001, la seguridad de la información implica evaluar riesgos para establecer los controles adecuados y verificarlos o medirlos.

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

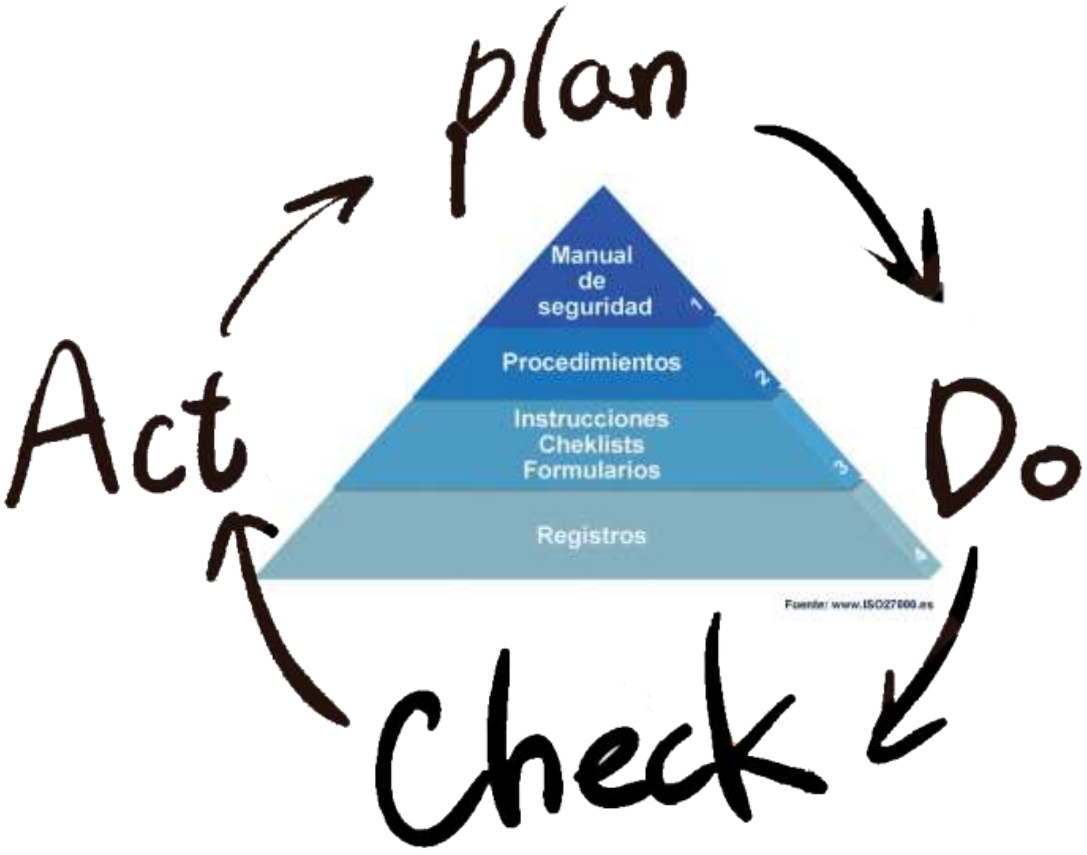
6.4.1 Generalidades ISO 27001

El establecimiento de un SGSI, de acuerdo a ISO 27001, implica:

- Determinar las necesidades y expectativas de los interesados (stakeholders).
- Establecer políticas y objetivos de la organización.
- Delimitar procesos y responsabilidades necesarias para lograr los objetivos.
- Escoger y aplicar métodos de medición de eficiencia y eficacia
- Determinar medios para prevenir las NO CONFORMIDADES
- Implementar el sistema con un enfoque de mejora continua.

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES



El SGSI conforme a ISO 27001 se puede trasladar al siguiente modelo:

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.4.2 Indicadores de gestión

Debido a que ISO 27001 establece que el SGSI debe implementarse en un esquema de mejora continua, este debe contar con indicadores que permitan verificar su efectividad.

Medir y evaluar los procesos de una organización nos otorga las herramientas necesarias para analizar, comprender y controlar mejor su funcionamiento, lo que a su vez nos permite predecir su comportamiento, así como mejorar su eficacia y eficiencia.

- **Medida:** proporciona una indicación cuantitativa de algún atributo de un proceso o producto.
- **Métrica:** Es una medida cuantitativa del grado en que un sistema, componente o proceso posee un atributo; permite comparar mediciones, medir objetivamente y evaluar y predecir.
- **Indicador:** Métrica o combinación de métricas que permiten conocer a profundidad el funcionamiento del proceso en su contexto.
- Los indicadores deben ser específicos, medibles, alcanzables, realistas y oportunos.

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.4.2 Indicadores de gestión

Los indicadores de gestión nos permiten conocer:

- Efectividad de los procesos de la organización/sistema
- Capacidad de la organización/sistema
- Estado de la organización/sistema
- Mejoras a los procesos de la organización/sistema

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.4.3 Esquema de implantación de un SGSI

ISO 27001 es un estándar que permite a cualquier organización, sin importar su tamaño, implantar su Sistema de Gestión de Seguridad de la Información, con base en las mejores prácticas internacionales.

Sin embargo, conseguir una implantación completa requiere de los conocimientos y concienciación de todos los involucrados, ya que esto facilitará o complicará el proceso.

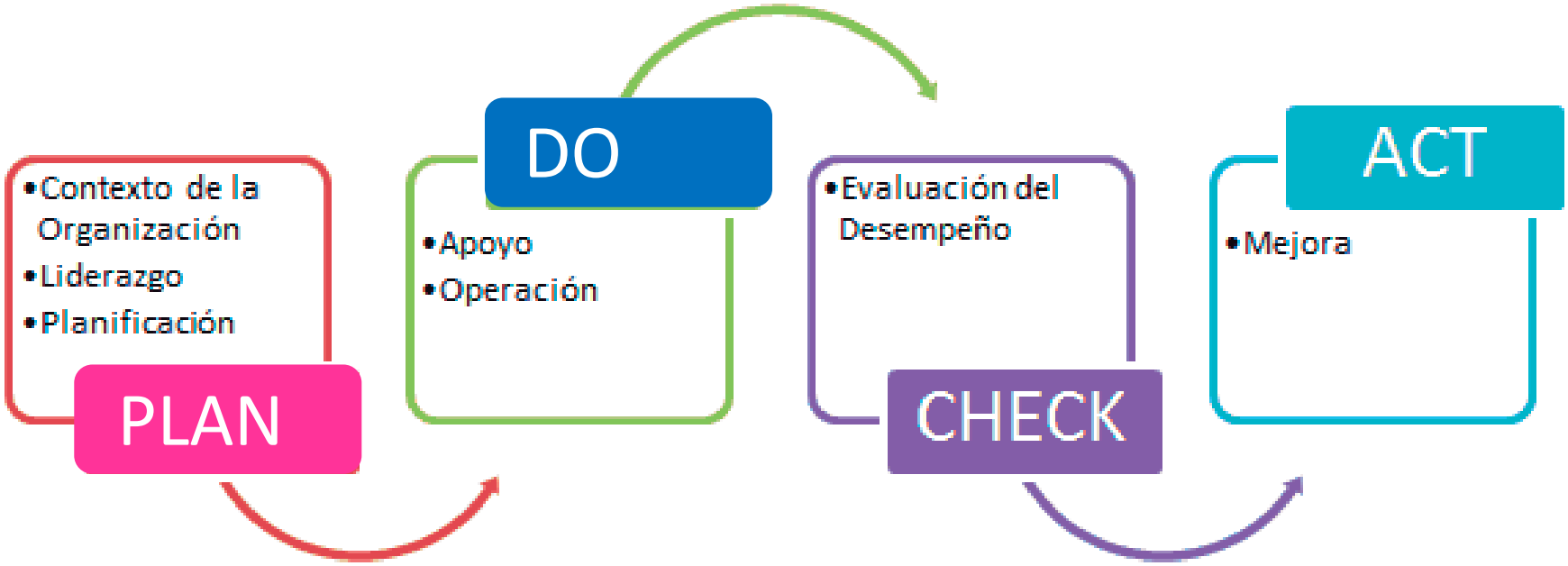
De forma general, se recomienda considerar los siguientes aspectos antes de iniciar el proceso de implantación:

- Contexto organizacional
- Liderazgo
- Planificación
- Soporte (apoyo)
- Operación
- Evaluación del desempeño
- Mejora continua

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.4.3 Esquema de implantación de un SGSI



6.4.3.1 Contexto organizacional

Conocer la organización:
comprender el modelo de negocio y los factores que influyen en la organización, sean internos o externos.

- **Conocer las necesidades y expectativas de los involucrados:**

identificar a los directamente involucrados en el SGSI, sean clientes o beneficiarios internos y externos, así como sus necesidades y expectativas.

- **Determinar el alcance:**

Considerando a la organización y sus involucrados, se debe definir con claridad el alcance, tomando en cuenta las dependencias entre las actividades internas y externas.

SGSI en Mejora Continua

6.4.3.2 Liderazgo

Compromiso:
Los objetivos del SGSI deben ser compatibles con los institucionales, garantizando recursos y asegurando los resultados; se debe impulsar desde la alta dirección.

Política:
Al menos se deben establecer directrices de gestión respecto a ser adecuada para la organización; se deben incluir los objetivos o proporcionar un marco para establecerlos e incluir el compromiso de satisfacer los requisitos y garantizar la mejora continua.

Funciones, responsabilidades y autoridad:
Determinar los miembros activos que formarán parte del funcionamiento del SGSI, con tareas claras, responsabilidades y autoridad necesaria.

Políticas

Las políticas organizacionales en materia de seguridad de la información, generales y/o específicas, deben derivarse de la alta dirección y:

- Contener la declaración de las reglas que se deben respetar para acceder a la información y los recursos.
- Desarrollarse con el fin de preservar la información, garantizando su confidencialidad, integridad y disponibilidad.
- Contemplar los procedimientos para hacer cumplir las reglas, la responsabilidad en todos los niveles y el apoyo gerencial explícito.
- Establecer claramente los objetivos, responsables de cumplimiento y medidas aplicables.

https://www.conicyt.cl/pia/files/2012/08/Politica-General-de-Seguridad-de-la-Informaci%C3%B3n-Conicyt-v211-rev-CS_14_07_2011.pdf

https://www.conicyt.cl/wp-content/uploads/2012/07/Politica-de-Gestion-de-Riesgos.pdf

6.4.3.3 Planificación

Acciones para enfrentar riesgos y oportunidades:

Debe asegurar el logro de resultados previniendo los efectos no deseados; considerar los asuntos internos y externos que influyen, así como les requisitos de todos los involucrados, que pueden convertirse en riesgos; establecer el plan de acción cuando se presente un riesgo o amenaza y documentar todo el proceso.

Objetivos de seguridad de la información y la planificación para alcanzarlos:

Se deben establecer objetivos según las funciones y niveles de los involucrados (en concordancia con la política), de forma medible y considerando los requisitos y necesidades.

Acciones para enfrentar riesgos y oportunidades

- Se debe asegurar que el SGSI logra resultados
- Se debe prevenir o reducir los efectos no deseados de la implantación
- Se debe lograr la mejora continua
- Se debe considerar los asuntos internos y externos y los requisitos de los interesados para identificar los riesgos potenciales, tomando en cuenta:
    - Identificar los propietarios del riesgo (el responsable del área afectada)
    - Analizar potenciales amenazas y probabilidades reales de ocurrencia, definiendo niveles de riesgo
    - Evaluar riesgos comparando con los resultados obtenidos
    - Priorizar acciones a realizar para reconducir la gestión del riesgo

- Se debe definir el proceso de tratamiento del riesgo en relación al plan, considerando:

Acciones para enfrentar riesgos y oportunidades

- Se debe definir el proceso de tratamiento del riesgo en relación al plan, considerando:
    - Seleccionar la opción de gestión del riesgo (prevenir, transferir, minimizar o aceptar).
    - Determinar los controles necesarios según la opción elegida.
    - Elaborar la planificación e implantación del tratamiento del riesgo.
    - Obtener una aprobación formal del propietario del riesgo, respecto a los riesgos residuales.
    - Documentar el proceso

Objetivos de seguridad de la información y planificación para alcanzarlos

Se deben establecer objetivos según las funciones y niveles de los involucrados (en concordancia con la política), de forma medible y considerando los requisitos y necesidades.

Para los objetivos, se debe determinar:

- ¿Qué hacer?
- ¿Qué recursos se necesitarán?
- ¿Quién será el responsable del seguimiento al objetivo?
- ¿Cuándo se alcanzará el objetivo?
- ¿Cómo se medirá el resultado?

6.4.3.4 Soporte

Recursos:
Determinar los mínimos necesarios, como el personal que opera y vigila el SGSI.

Competencias:
Los responsables de operar el SGSI deben tener los conocimientos y recursos que les permitan ser competentes y evidenciar este proceso.

Concienciación:
El personal debe ser consciente de la política de seguridad, su contribución al SGSI y su implicación en la resolución de No conformidades.

Comunicación:
Formalizar las vías de comunicación e identificar las necesidades internas y externas al respecto.

Documentación:
La organización determina los documentos necesarios que hacen efectivo el SGSI, considerando los mínimos indispensables.

Comunicación

Se deben formalizar las vías de comunicación e identificar las necesidades internas y externas de esta. Para ello, se debe considerar:

¿Qué se debe comunicar?
¿Cuándo se debe comunicar?
¿A quién se debe comunicar?
¿Quién debe comunicar?
¿Cuál es el proceso de comunicación?

Aspectos relevantes, sobre todo ante la ocurrencia de incidentes

Documentación

La organización puede determinar los documentos que considere necesarios y que integrarán el SGSI para hacerlo efectivo, sin embargo debe considerar los mínimos necesarios tomando en cuenta:

- Tamaño y tipo de la organización
- Actividades y productos o servicios
- Complejidad de sus procesos o interacciones
- Competencia de las personas involucradas

La documentación que se determine, debe:

- Estar accesible y ser adecuada para su uso
- Estar debidamente protegida
- Tener controles de cambios

6.4.3.5 Operación

Planificación y control operacional:
Planificar, implementar y controlar los procesos necesarios e implementar acciones necesarias para gestionar el riesgo.

Evaluación de los riesgos de seguridad de la información:
Se debe realizar el proceso de identificación y análisis de riesgos de forma planificada y a intervalos establecidos o cuando ocurran cambios, permitiendo ajustar la planificación.

Tratamiento de los riesgos de seguridad de la información:
Conforme se implanta el plan de tratamiento de riesgos, se modifican los criterios de operación y se actualizan nuevamente los planes.

6.4.3.6 Evaluación del desempeño

Control, medición, análisis y evaluación:
¿Qué se debe controlar?, ¿cuáles métodos de evaluación, control y medición se utilizarán?, ¿con qué frecuencia se evaluará?, ¿quién realizará los controles y la medición?, ¿cuándo se evalúan y analizan los resultados?

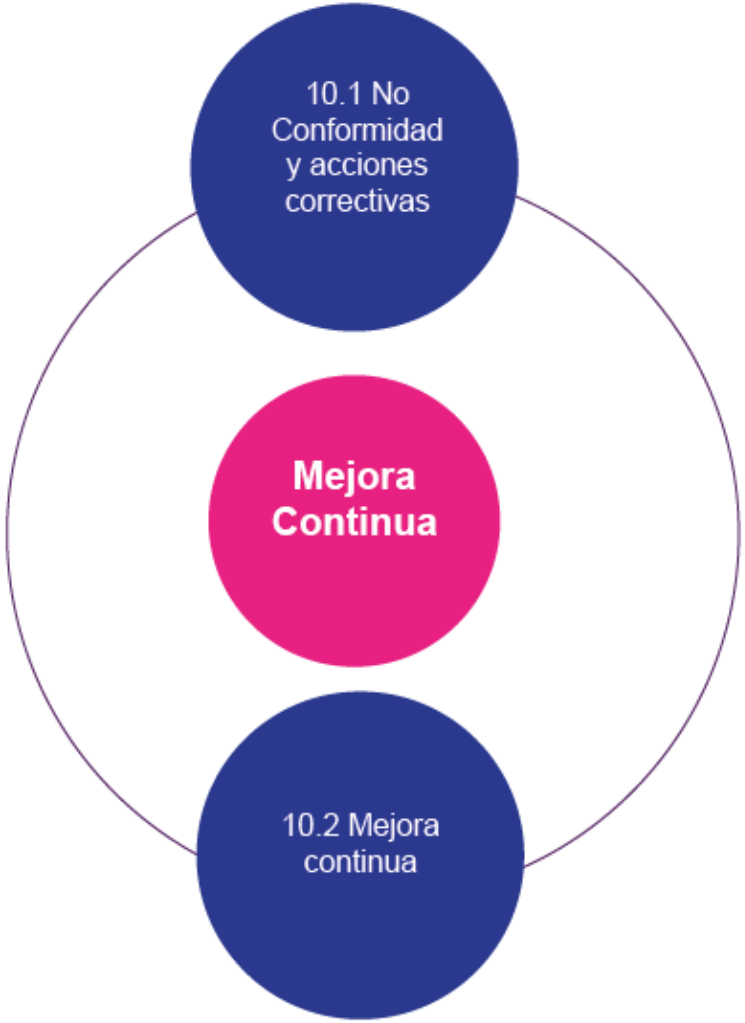
Auditoría interna planificada:
Permite evaluar si el SGSI se ha implementado y se mantiene de forma efectiva; si es conforme a los requisitos de la propia organización y el estándar; si está implantado y mantenido eficientemente.

Revisión por la alta dirección:
La alta dirección debe revisar el estado del SGSI y sus procesos, para asegurar su mejora continua.

Revisión por la alta dirección

La alta dirección debe revisar el estado del SGSI y sus procesos, para asegurar su mejora continua. Para ello, debe revisar:

- Estado de acciones y revisiones anteriores.
- Cambios relevantes.
- Retroalimentación del rendimiento, incluyendo estadísticas sobre:
  - No conformidades
  - Correcciones
  - Monitoreo y resultados
  - Cumplimiento de objetivos
- Retroalimentación de los interesados
- Resultados del análisis de riesgos y el estado del plan de tratamiento
- Oportunidades de mejora



6.4.3.7 Mejora continua

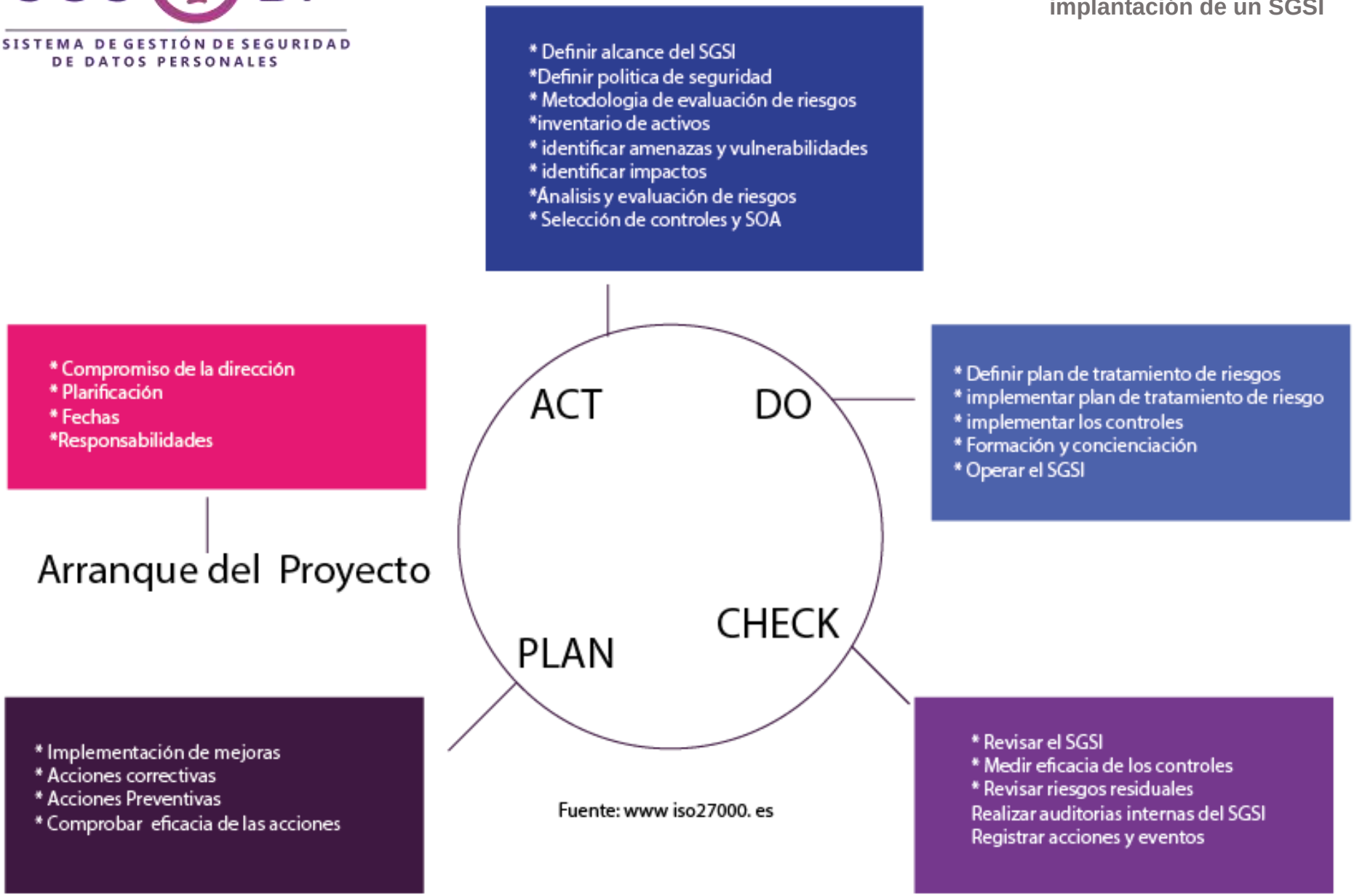
No conformidad y acciones correctivas:
Reacciones frente a las no conformidades presentadas, las acciones de corrección y control, el manejo de consecuencias; la eliminación de las causas de la no conformidad y potenciales nuevas ocurrencias.

Mejora continua y acciones preventivas

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.4.3 Esquema de implantación de un SGSI



Fuente: www iso27000. es

SGS DP

SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.5 Recomendaciones de implantación del SGSDP

El artículo 44 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Morelos (LPDPPSOEM), establecen la obligación de contar con un sistema de gestión y define los alcances del mismo.

Implementar un SGSDP en un Sujeto Obligado es una tarea compleja y de mucho trabajo al interior; requiere, para empezar, del compromiso desde la alta dirección, ya que se necesita adaptar muchos procesos y procedimientos internos y en algunos casos, implica el cambio de mentalidad de los involucrados hacia un enfoque que coloca en el centro la seguridad de la información de las personas.

SGS DP
SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.5.1 Contexto organizacional

El titular del Sujeto Obligado (SO) debe determinar quién será la persona o grupo de trabajo responsable de implementar el Sistema de Gestión de Seguridad de Datos Personales (SGSDP).

La LPDPPSOEM establece que el oficial de datos deberá realizar las atribuciones específicas en materia de protección de datos personales, sin embargo, como hemos visto, el Sistema de Gestión de Seguridad de Datos Personales es más amplio, por lo que se sugiere involucrar a las áreas que puedan reforzar esta tarea, siempre en función de la capacidad del Sujeto Obligado.

El equipo o persona designado para implantar el SGSDP en el SO, deberá tener conocimiento y dominio de los objetivos y procesos institucionales, así como de las necesidades y expectativas de los involucrados.

La alta dirección, en conjunto con el responsable de la implantación, deberán definir el alcance que tendrá el SGSDP, el cual bien podría desarrollarse en etapas.

SGS DP
SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.5.2 Identificación de los interesados

El responsable de la implantación del SGSDP debe identificar a todos los interesados, ya que de ello dependerá el éxito en la implantación.

Se debe considerar:

El personal del Sujeto Obligado
El personal que trata datos personales
Los proveedores
Los Encargados de tratamiento
Los receptores de transferencias
Los titulares de los datos
Los clientes o usuarios
Interesados indirectos

De ellos, se debe identificar sus expectativas y necesidades, ya que no todos requerirán lo mismo para poder involucrarse en la implantación ni tendrán las mismas expectativas del proceso.

Una inadecuada identificación de interesados y expectativas, puede derivar en una implantación fallida, lo que dificultará aún más una implantación posterior.

6.5.3 Identificación de requerimientos

El responsable de la implantación del SGSDP debe identificar todos los requerimientos necesarios para lograr el éxito en el proyecto.

Estos requerimientos deben incluir los económicos, materiales, humanos, de conocimiento y de comunicación.

Se debe definir los requerimientos mínimos necesarios que permitan la implantación, para evitar que la solicitud de recursos elevados se vuelva un obstáculo institucional.

El liderazgo del responsable de la implantación será un factor fundamental, ya que se debe hacer conciencia en la alta dirección de la importancia de implantar el SGSDP de manera correcta y efectiva; para ello, el responsable puede generar sinergia con involucrados externos y fomentar la concienciación con los involucrados internos.

6.5.4 Planificación de la implantación

El responsable de la implantación del SGSDP debe establecer un plan de trabajo que incluya:

- Recursos materiales
- Recursos financieros
- Recursos humanos
- Tiempo o plazos (hitos)
- Indicadores
- Reportes

Para planificar la implantación, debe considerar a todos los involucrados, su nivel de compromiso y su grado de competencia, así como la complejidad de sus procesos internos.

La comunicación efectiva del plan a todos los involucrados es parte fundamental del éxito en la implantación.

6.5.5 Evaluación y monitoreo

El responsable de la implantación del SGSDP debe establecer los medios de verificación del grado de cumplimiento, teniendo como base el alcance determinado en conjunto con la alta dirección.

Una vez iniciada la implantación, deberá monitorear los indicadores establecidos para verificar su cumplimiento y poder evaluar el proceso de implantación.

Es importante que estas evaluaciones de planifiquen y efectúen de manera oportuna, durante el curso de la implantación, para poder realizar las correcciones a tiempo y asegurar el éxito del proceso.

No debe perderse de vista que, en ocasiones, alcanzar resultados aparentemente favorables, puede ocultar incidencias que a la larga afecten a la institución, por ello el responsable de la implantación debe realizar una evaluación minuciosa.

SGS DP
SISTEMA DE GESTIÓN DE SEGURIDAD DE DATOS PERSONALES

6.5.6 Mejora continua

El responsable de la implantación del SGSDP debe reaccionar oportunamente con base en los resultados de las verificaciones y monitoreo.

En caso de que se tengan resultados negativos o menores a los esperados, deberá proponer e implementar, previa aprobación de la alta dirección, medidas correctivas que aseguren la consecución de los objetivos.

En caso de que se tengan resultados positivos mayores a los esperados, deberá también proponer e implementar, previa autorización de la alta dirección, medidas que fortalezcan el proceso.

Gracias