Módulo 2

Gestión de Seguridad de la Información

PRIME CONSULTORES

I. Marco Regulatorio

a. Circular Nº 140

Finalidad

Las mencionadas empresas deben **establecer, mantener y documentar** un Sistema de Gestión de la Seguridad de la Información (SGSI), teniendo en cuenta las siguientes actividades mínimas :

- Definición de una política de seguridad de información aprobada por el Directorio.
- Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.
- Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

I. Marco Regulatorio

b. ISO 27001: En resumen

¿Qué es la Norma ISO 27001

Sistema de Gestión de Seguridad de la Información (SGSI)

Es un Modelo para establecer, implementar, monitorear, mantener y mejorar un SGSI bajo un enfoque basado en procesos. La adopción de un SGSI debe ser una decisión estratégica para la Institución.

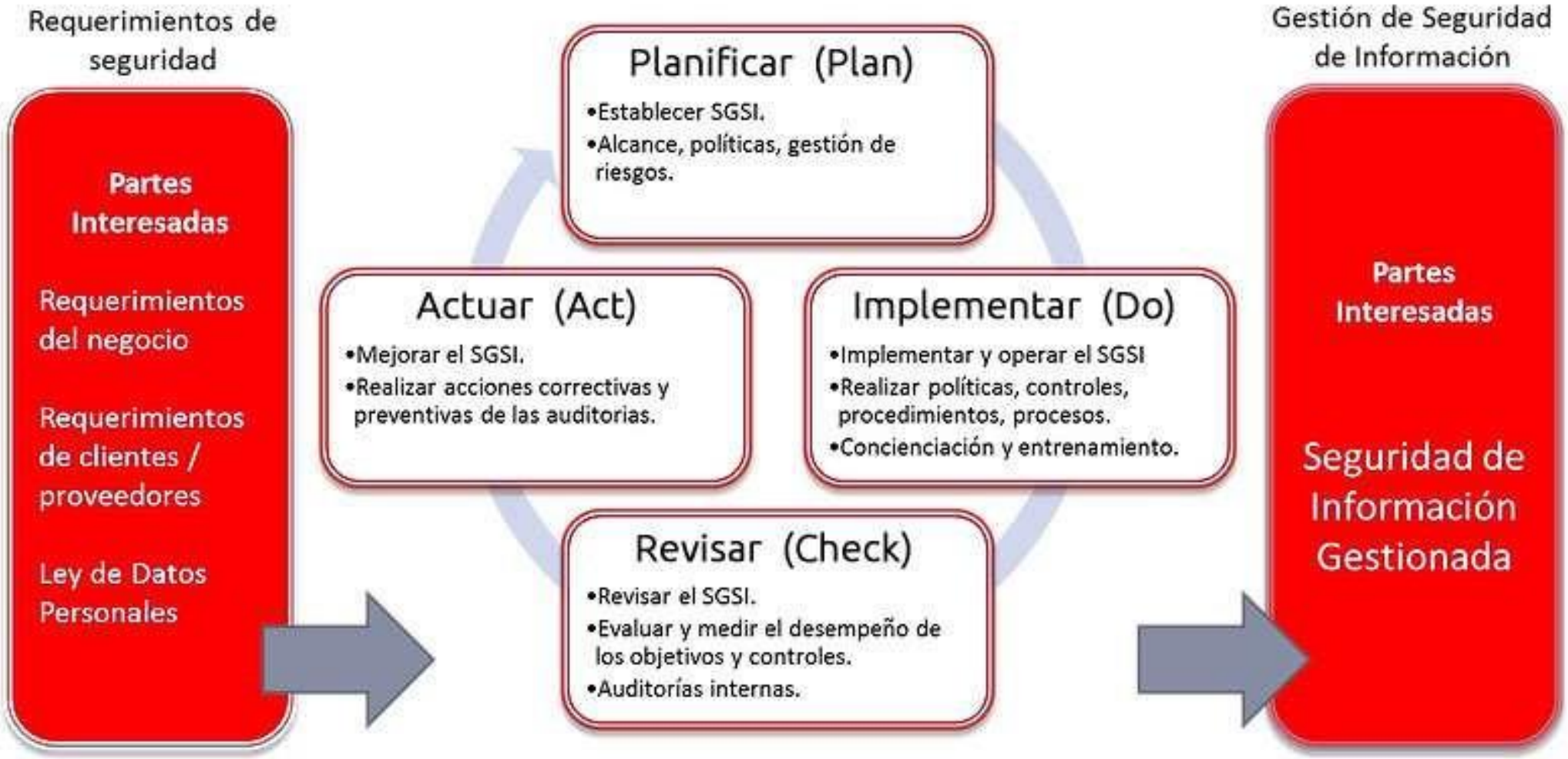
El "enfoque basado en procesos" estimula al personal pa que pongan énfasis en la importancia de:

- ✓ Comprender los requisitos de seguridad de la informaci de su organización.
- ✓ Implementar y operar controles para gestionar los riesgos de seguridad de la información.
- ✓ Monitorear y revisar el desempeño y eficacia del SGSI.
- ✓ La Mejora continua en base a la medición de objetivos.

Sistema de Gestión de Seguridad de la Información
(Ciclo "Deming")

I. Marco Regulatorio

b. ISO 27001: En resumen



II. Fase de Planificación

Conceptos Básicos

Objetivo de la Seguridad de Información

- Encargada de proteger la información de un amplio rango de amenazas con la finalidad de:
  - Asegurar la continuidad de las operaciones de la Institución
  - Minimizar los daños a la organización en caso de pérdida o revelación no autorizada de información.
  - Mantener la imagen institucional

II. Fase de Planificación

Conceptos Básicos

II. Fase de Planificación

Conceptos Básicos

Terminología en Seguridad de la Información

- Activo de Información
- Amenaza
- Vulnerabilidad
- Riesgo
- Exposición
- Salvaguarda
- Impacto

PRIME CONSULTORE

II. Fase de Planificación

Conceptos Básicos

SUBGERENCIA DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO

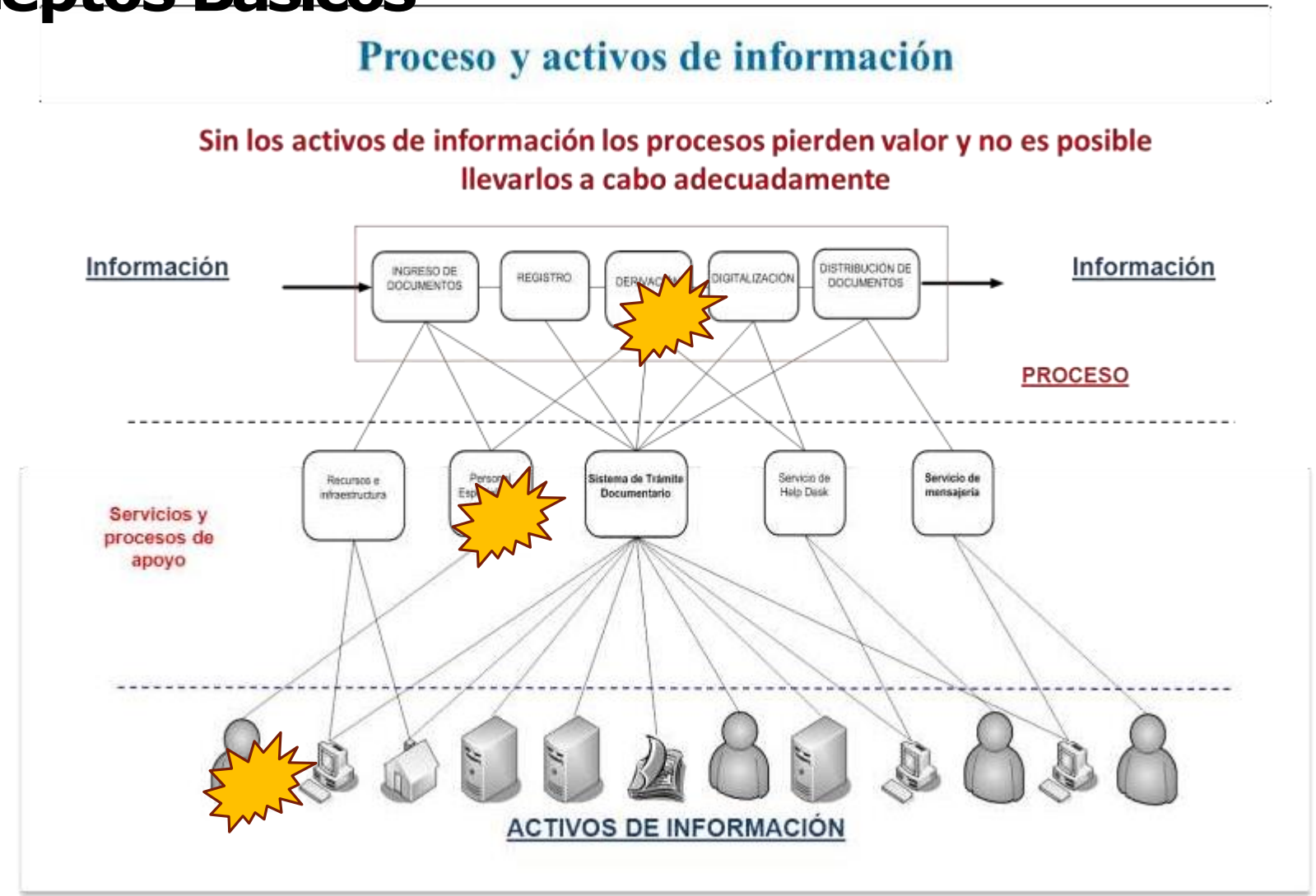
Activos de Información

Se denomina activo de información a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información.

PRIME CONSULTORES

II. Fase de Planificación

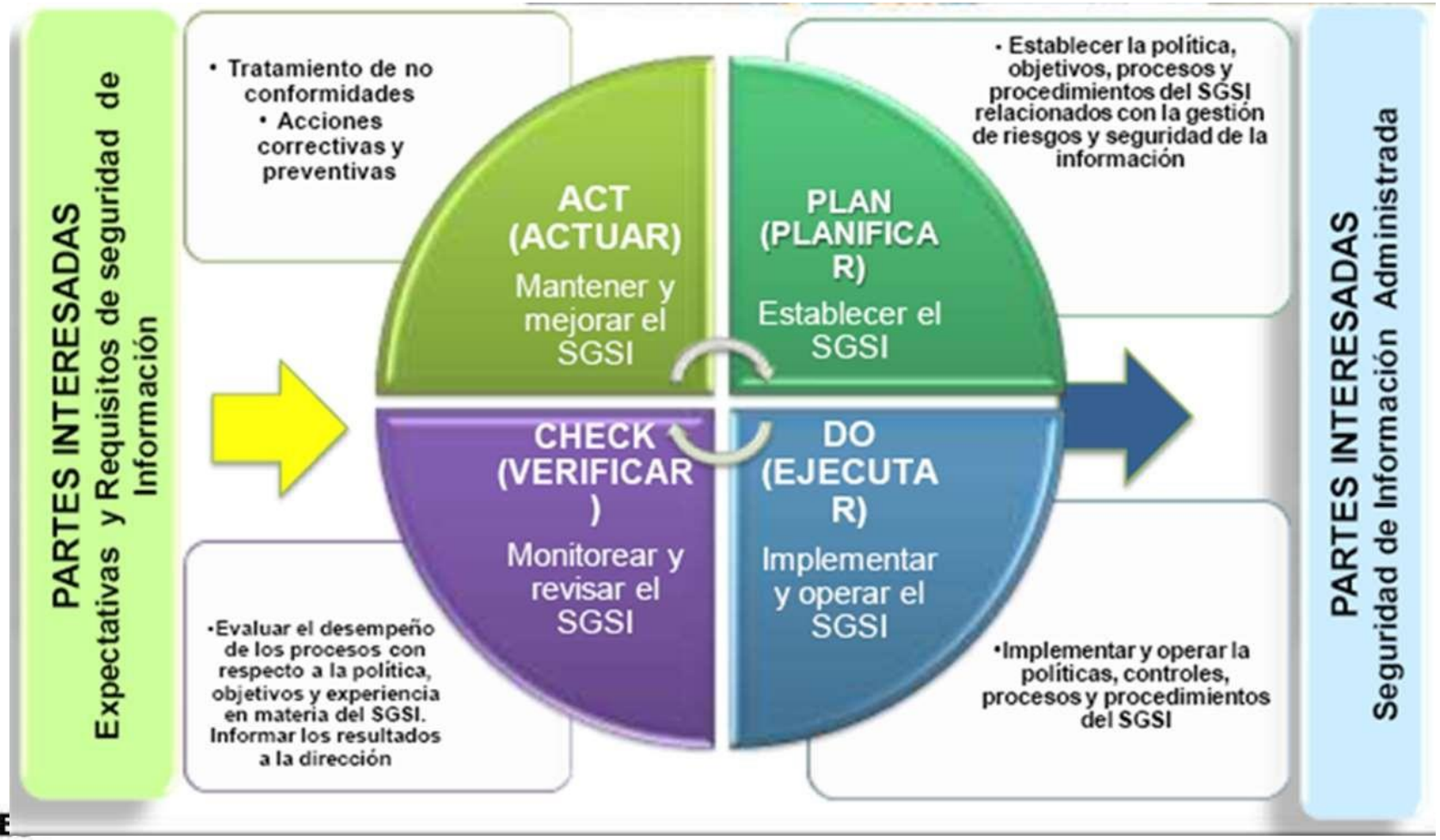
Conceptos Básicos



PRIME CONSULTORES

II. Fase de Planificación

a. Fase de Planificación: Establecimiento del SGSI



II. Fase de Planificación

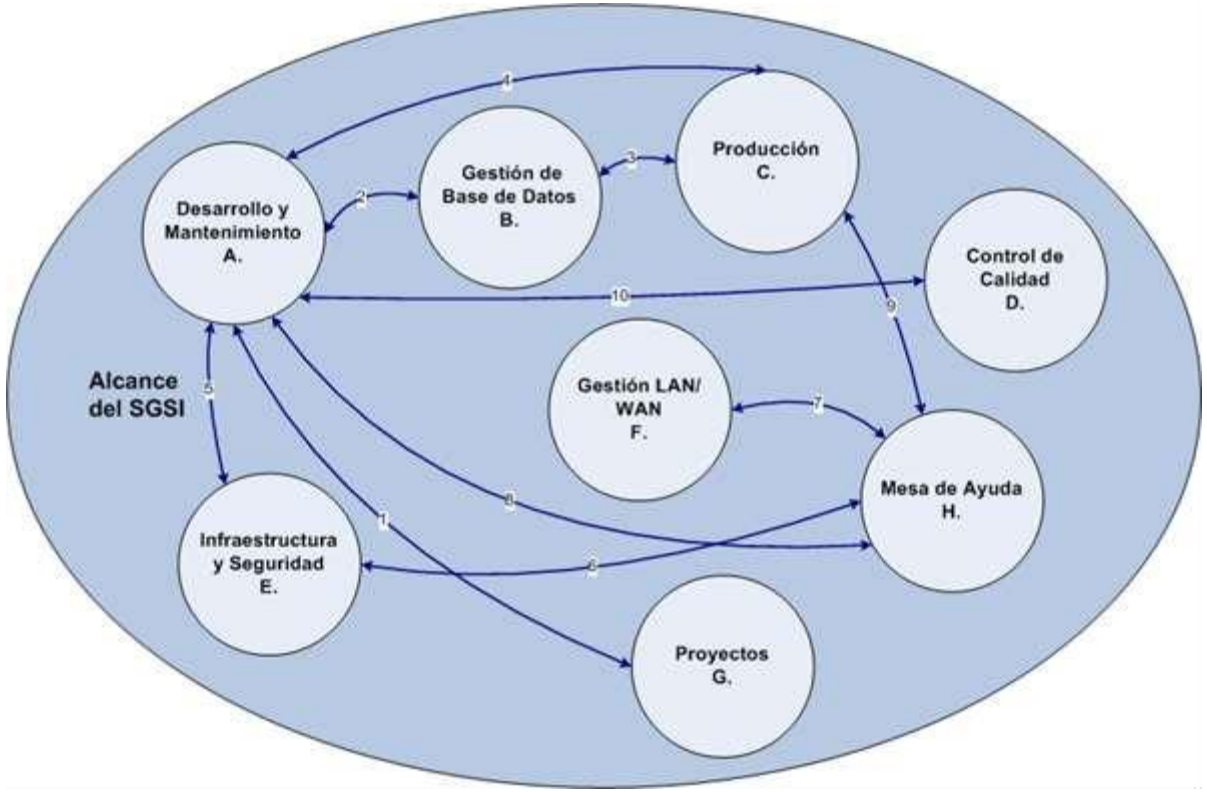
a. Fase de Planificación: Establecimiento del SGSI

PLANIFICAR
(establecer el SGSI)

- Definición del alcance y límites de SGSI
- Definir la Política del SGSI
- Realizar el Análisis y Evaluación de Riesgos
- Establecer las Opciones para el Tratamiento de Riesgos
- Definir las políticas y procedimientos de seguridad y del SGSI
- Obtener la aprobación y autorización de la dirección para implementar el SGSI
- Establecer el SOA (Declaración de Aplicabilidad)

II. Fase de Planificación

c. Definición de alcance



PRIME CONSULTORES

II. Fase de Planificación

d. Redacción de la Política

Política de Seguridad de Información

OBJETIVO: Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones

- La gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y mantenimiento una política de seguridad en toda la organización.

PRIME CONSULTORES

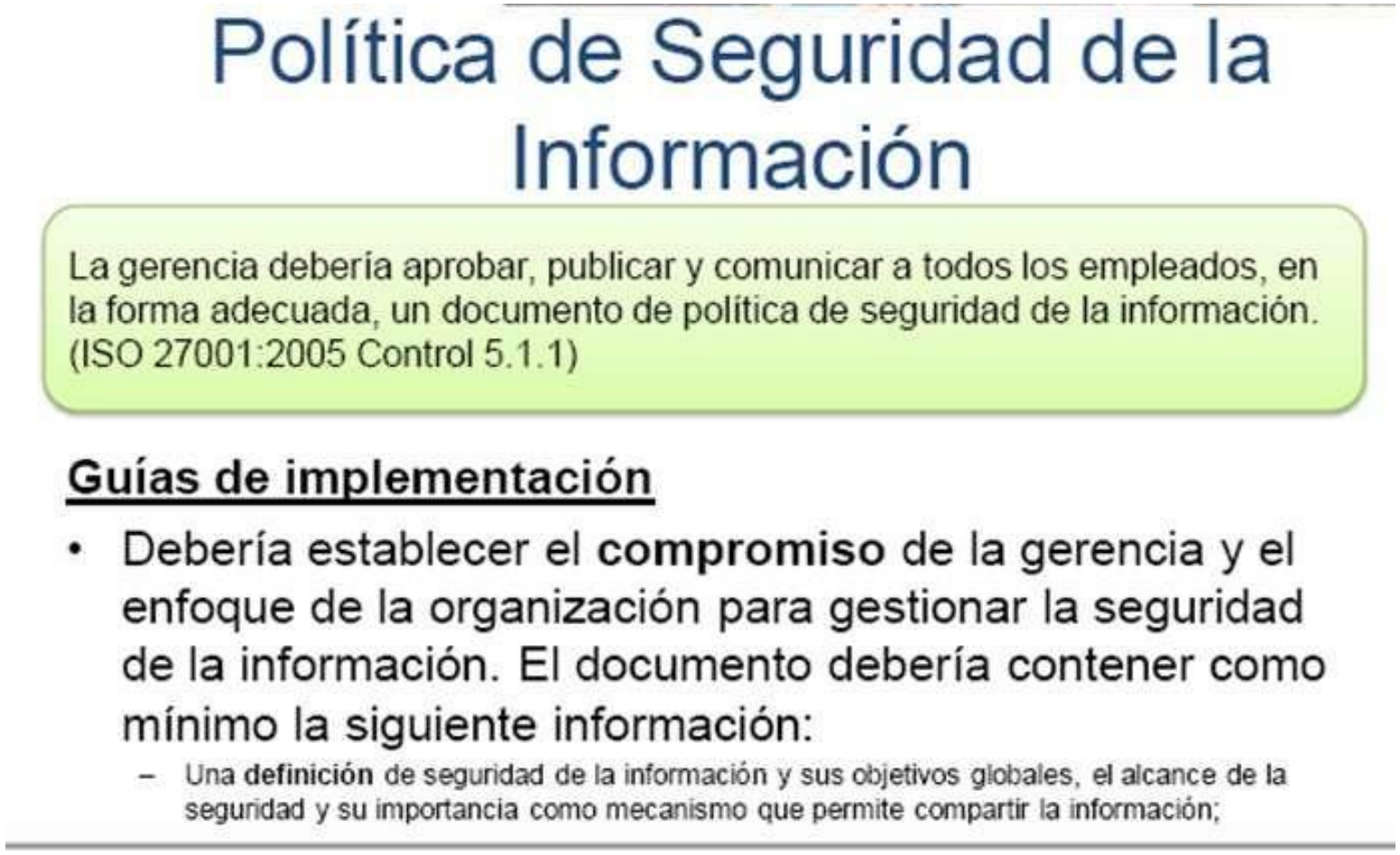
II. Fase de Planificación

d. Redacción de la Política

Consideraciones para el diseño de las políticas de seguridad

II. Fase de Planificación

d. Redacción de la Política



II. Fase de Planificación

e. Definición del enfoque de evaluación de riesgo

PRIME CONSULTORES

II. Fase de Planificación

f. Procedimiento para la evaluación de riesgo

Inventario de Activos

- Relación de todos los activos importantes
- Cada activo debe tener un dueño (Responsabilidades definidas)
- Los activos se identifican, no se inventan

"La información debe protegerse cualquiera que sea la forma que tome o los medios por los que se comparta o almacene".

NTP ISO/IEC 17799:2007

No confundir con activos fijos

PRIME CONSULTORES

II. Fase de Planificación

f. Procedimiento para la evaluación de riesgo

Amenazas

- Causa potencial de un incidente no deseado que puede resultar en daño al sistema o a la organización o a sus activos
- Puede ser accidental o intencional
- Los activos están sujetos a muchos tipos de amenazas que explotan sus vulnerabilidades:
  - **Desastres naturales**: terremoto, inundación, etc.
  - **Humanas**: errores de mantenimiento, huelga, errores de usuario
  - **Tecnológicas**: caída de red, sobre tráfico, falla de hardware

II. Fase de Planificación

f. Procedimiento para la evaluación de riesgo

Vulnerabilidades

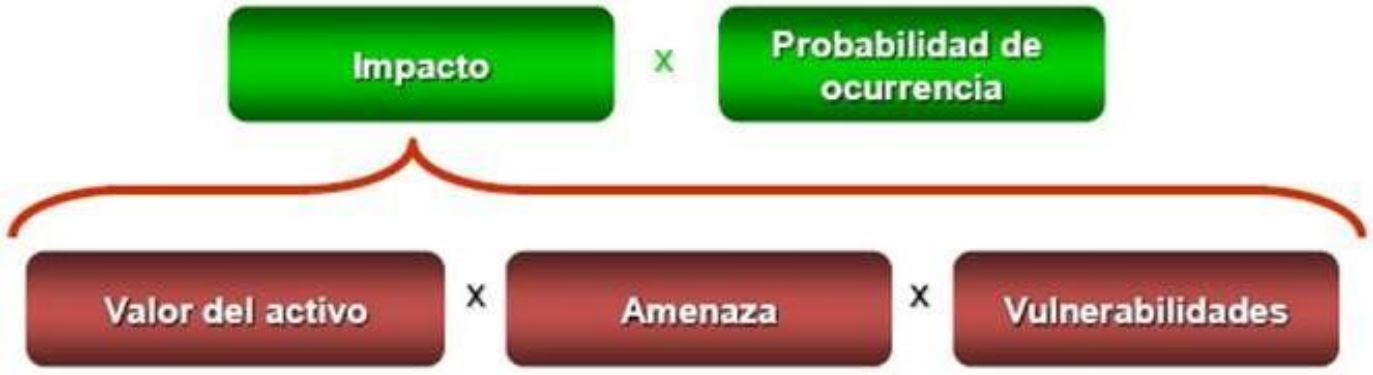
- Una vulnerabilidad es una debilidad o ausencia de control en la seguridad de información de una organización
- Por sí sola no causa daños
- Si no es administrada, permitirá que una amenaza se concrete
- Ejemplo:
  - Ausencia de personal clave
  - Sistema de energía inestable
  - Cableado desprotegido
  - Falta de conciencia de seguridad
  - Ausencia de sistema extinguidor de incendios

II. Fase de Planificación

f. Procedimiento para la evaluación de riesgo

Riesgo

Un Riesgo de Seguridad es el potencial de que una amenaza determinada pueda explotar las vulnerabilidades de un activo o grupo de activos de información para causar pérdidas o daños



PRIME CONSULTORES

II. Fase de Planificación

f. Procedimiento para la evaluación de riesgo

- ¿Qué herramientas recomienda la norma?
  - La norma no indica el uso de una herramienta específica.
- La evaluación de riesgo debe identificar los activos, las amenazas, vulnerabilidades, la probabilidad de ocurrencia y el impacto que puede tener en la organización, determinando así el nivel de riesgo efectivo.
- Lo importante en los procesos de evaluación de riesgos es que se establezca un adecuado tratamiento a los riesgos identificados.
- Debe contener por lo menos:
  - Colección de datos
  - Análisis
  - Salida de resultados

II. Fase de Planificación

g. Realización del tratamiento de riesgo

II. Fase de Planificación

g. Realización del tratamiento de riesgo

OPCIONES

- **Aceptar** el riesgo efectivo
- **Transferir** el riesgo
- **Reducir** el riesgo a un nivel aceptable
- **Evitar** Riesgos

II. Fase de Planificación

g. Realización del tratamiento de riesgo

TIPOS DE CONTROL

- **Controles Técnicos**:
  - Supresión de fuego/sistemas rociadores
  - Sistemas de control de acceso
  - Guardias de seguridad
- **Controles Documentales**:
  - Políticas de contratación y terminación
  - Política de escritorios limpios
  - Recepción de documentos
- **Controles Organizacionales**:
  - Conformación de Comité de Seguridad
  - Oficial de Seguridad
  - Capacitación del Personal

II. Fase de Planificación

g. Realización del tratamiento de riesgo

Nivel de riesgo aceptable

- No es posible conseguir seguridad total al 100% ó 0% de Riesgos
- Siempre existirán riesgos residuales
- ¿Cuál es el nivel de riesgo residual aceptable en la organización?
  - La alta dirección debe decidir

II. Fase de Planificación

g. Realización del tratamiento de riesgo

Tratamiento del Riesgo

- La decisión dependerá de:
  - Ubicación del activo
  - Seguridad existente
  - Número de atacantes
  - Instalaciones disponibles
  - Nivel de exposición
  - Planeamiento de la continuidad de negocios

II. Fase de Planificación

g. Realización del tratamiento de riesgo

TRATAMIENTO DEL RIESGO

- Definir un nivel aceptable de riesgos residuales
  - Revisar constantemente las amenazas y vulnerabilidades
  - Revisar los controles de seguridad existentes
  - Aplicar controles de seguridad adicionales
  - Introducir política y procedimientos
  - Selección de controles

PRIME CONSULTORES

II. Fase de Planificación

g. Realización del tratamiento de riesgo

Plan de Tratamiento de Riesgos

Plan de Acción que define las acciones para reducir los riesgos no aceptables e implementar los controles necesarios para proteger la información.

PRIME CONSULTORE

II. Fase de Planificación

g. Realización del tratamiento de riesgo

Facilidades de implementación

- ¿El ambiente apoya el control?
- ¿Cuánto tiempo tomará implementar el control?
- ¿El control está disponible de inmediato?

PRIME CONSULTORES

II. Fase de Planificación

h. Declaración de aplicabilidad

Definición de SOA

- Declaración documentada que describe los objetivos de control y controles que son pertinentes y aplicables al SGSI que se implementará en la Institución

- Nota: los objetivos de control y controles se basan en los resultados y conclusiones de los procesos de evaluación y tratamiento del riesgo, los requisitos legales o reglamentarios, las obligaciones contractuales para la seguridad de la información

II. Fase de Planificación

h. Declaración de aplicabilidad

DOMINIOS DE LA NORMA ISO 27001

PRIME CONSULTORES

III. Implementación del SGSI-Fase DO

a. Plan de tratamiento

Objetivos que persigue la Implementación del SGSI:

- **Implantar el conjunto de controles desarrollados** (políticas, procedimientos, instructivos de Seguridad de la Información) en la Institución.
- **Lograr la participación de todo el personal**, utilizando los controles desarrollados como parte de sus actividades cotidianas dentro de la Institución y en base a las funciones que desempeña.
- **Establecer la participación activa de la Alta Dirección** para lograr los recursos y el apoyo necesario requerido para su implantación.
- **Permitir la operación del SGSI** elaborado.
- **Poner en práctica las funciones y responsabilidades de los** Comités y del personal para gestionar la Seguridad de la Información.

III. Implementación del SGSI-Fase DO

a. Implementación del SGSI

La organización debe realizar lo siguiente:

a) **Formular un Plan de Tratamiento de Riesgos:** que permita identificar las acciones requeridas para gestionar los riesgos de seguridad de la información en la Institución.

b) **Implementar el Plan de Tratamiento de Riesgos:** que permita cumplir con los objetivos de control identificados en materia de seguridad de la información.

c) **Definir como medir la eficacia de los controles o grupos de controles seleccionados:** que permita conocer como utilizar estas mediciones para evaluar la eficacia del control implementado.

d) **Implementar programas de capacitación en Seguridad de la Información para el personal:** que permita dar a conocer las amenazas existentes actuales y las formas de controlar el riesgo, buscando la concientización del personal.

PRIME CONSULTORES

III. Implementación del SGSI-Fase DO

b. Recursos documentación y medición

e) **Gestionar la Operación del SGSI:** que permita poner en funcionamiento el modelo de Seguridad de la Información desarrollado.

f) **Gestionar los Recursos para el SGSI:** que permita establecer, implementar, operar y mejorar el Sistema de Gestión de Seguridad elaborado.

g) **Implementar procedimientos y otros controles para la detección y respuesta ante incidentes de seguridad:** que permita establecer las acciones a seguir para responder efectivamente ante la presencia de un incidente o hecho que pueda impactar en las operaciones de la Institución.

III. Implementación del SGSI-Fase DO

c. Organización de la seguridad de la información

PRIME CONSULTORES

III. Implementación del SGSI-Fase DO

d. Dominios

DOMINIOS DE LA NORMA ISO 27001

III. Implementación del SGSI-Fase DO

e. Continuidad del negocio

PRIME CONSULTORES

Gracias

Econ. Yuri Luna C.
Gerente de Proyectos de Consultoría
ORM – ISO 31000 Lead Risk Manager
ISO 22301 Lead Implementador
ISO 27001 Lead Implementador
PRIME Consultores