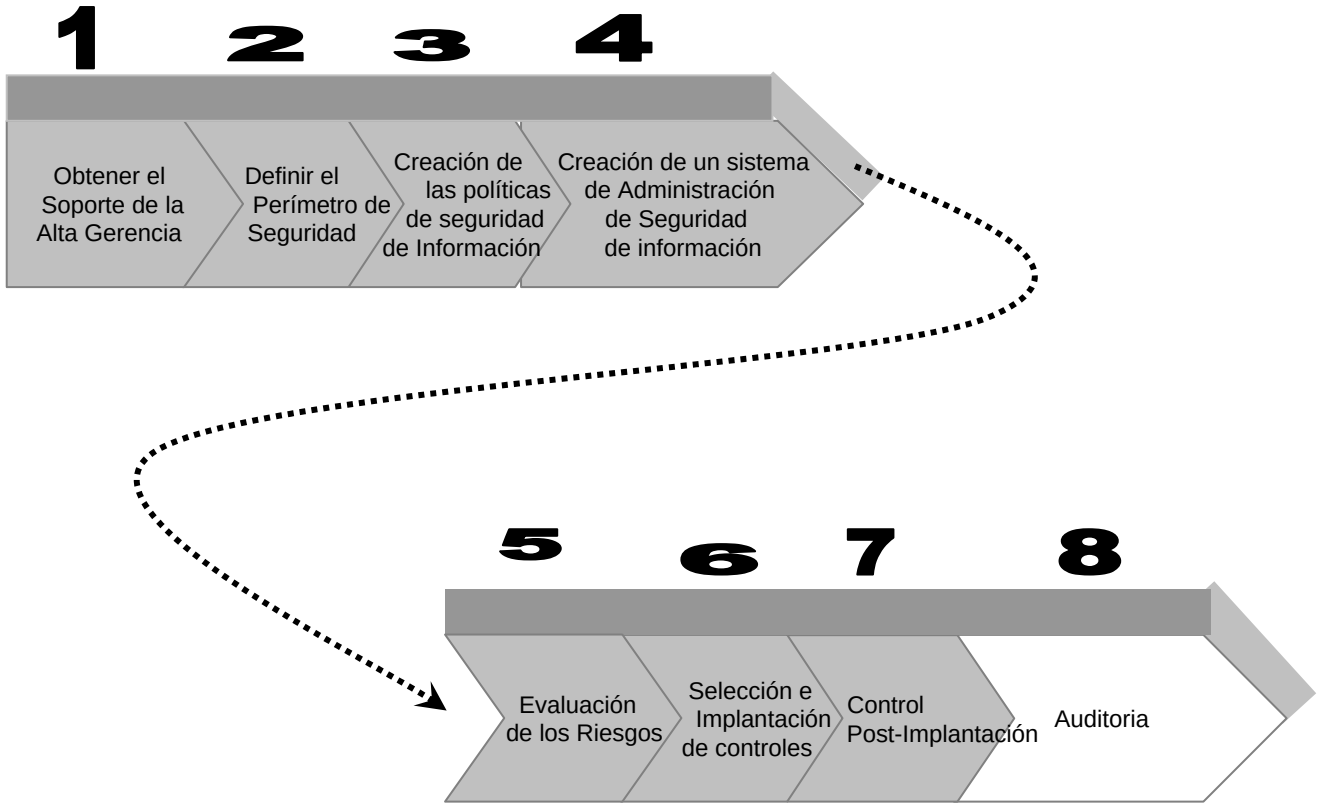
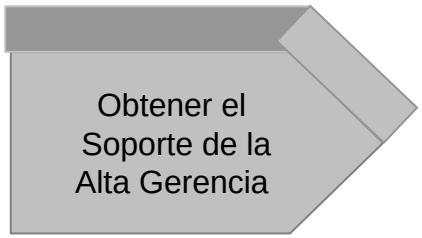
Metodología para Implantar BS-7799 en una empresa


1
2
3
4
Obtener el Soporte de la Alta Gerencia
Definir el Perímetro de Seguridad
Creación de las políticas de seguridad de Información
Creación de un sistema de Administración de Seguridad de información
5
6
7
8
Evaluación de los Riesgos
Selección e Implantación de controles
Control Post-Implantación
Auditoria

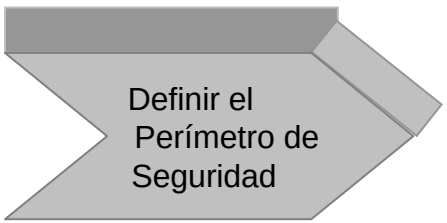
Aplicando el ISO 17799: paso a paso

1



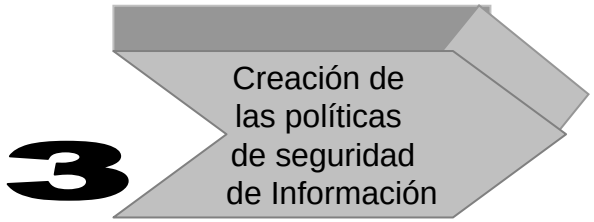
- Lo mas importante para el éxito de la implementación del ISO 17799 es el soporte de la Alta Gerencia
- La seguridad de información no es un programa, es un proceso

2

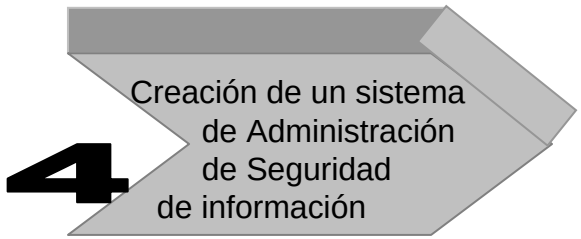


- Una de las tareas mas complicadas es la definición del perímetro de la seguridad
- El alcance de la seguridad puede o no englobar a toda la organización

Aplicando el ISO 17799: paso a paso

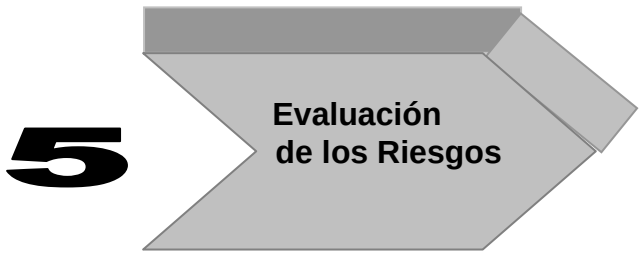


- Las políticas pueden adoptar diversas formas
- Deben indicar el marco de referencia de la seguridad para la organización, en términos de conceptos y de objetos



- Es necesario implementar, administrar, mantener y velar por el cumplimiento de los procesos de seguridad de información
- El ISMS define el alcance y provee una guía detallada de las estrategias de seguridad de información para todas las áreas de control del ISO 17799

Aplicando el ISO 17799: paso a paso



Los pasos que efectuamos para evaluar los riesgos son los siguientes:

- Identificar los activos dentro del perímetro de la seguridad
- Identificar las amenazas sobre los activos
- Identificar las vulnerabilidades de los activos
- Determinar la probabilidad de ocurrencia
- Calcular el impacto
- Calcular el riesgo

Un riesgo no puede ser mitigado si no ha sido identificado

Aplicando el ISO 17799: paso a paso

- Establecer un mapa de los procesos de negocio
- Determinar los procesos críticos de negocio
  - Mapear cada proceso.
  - Identificar los activos de información que soportan cada proceso.
- Realizar la clasificación de información y realizar la evaluación de riesgos de dichos procesos críticos

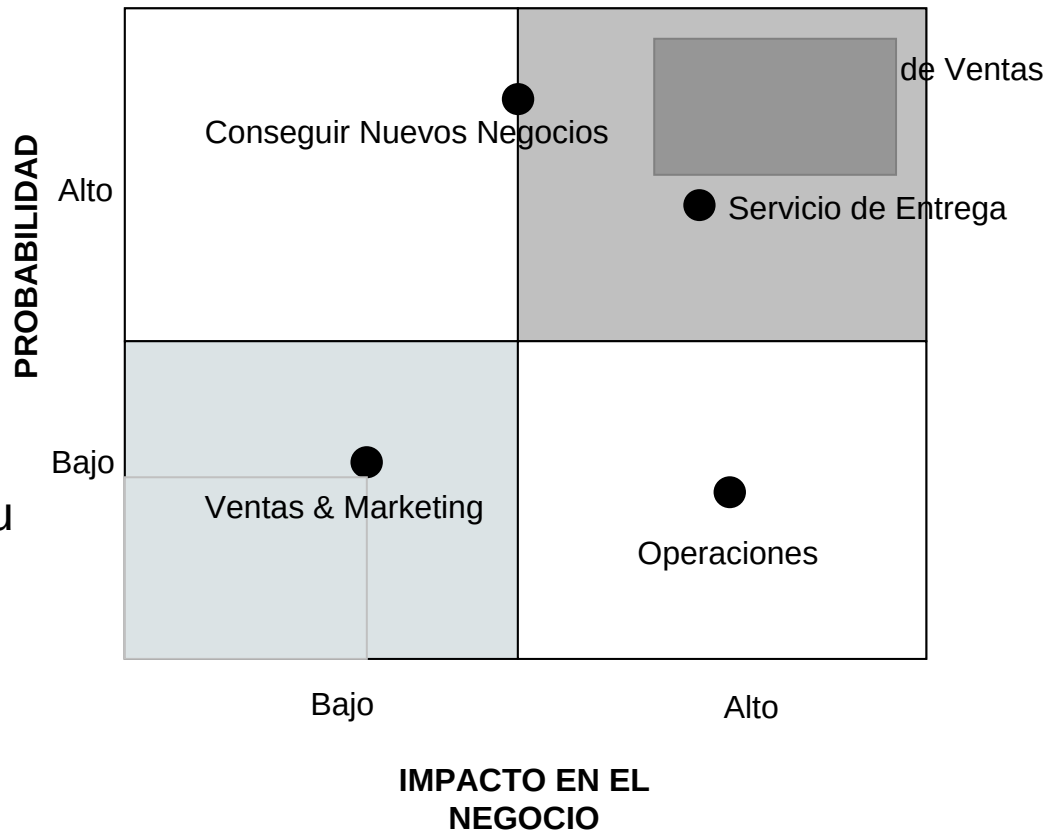
Evaluación de los Riesgos
Basados en los procesos claves del negocio

Probabilidad-

La probabilidad de ocurrencia y duración en el caso de ocurrir una pérdida o daño.

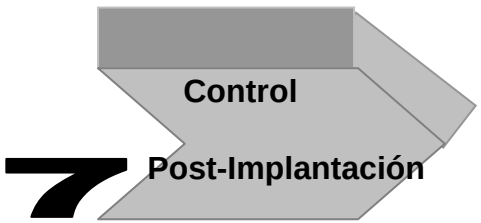
Impacto en el Negocio-

El grado de pérdida o daño potencial la capacidad financiera u operacional dentro del proceso del negocio.



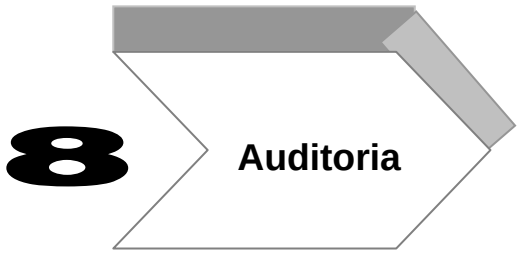
Aplicando el ISO 17799: paso a paso (Cont.)

- Los controle mitigan el riesgo que ha sido identificado previamente
- Los controles pueden ser priorizados de acuerdo al valor del riesgo.



- Es la porción del ISMS que documenta como los riesgos identificados son mitigados por los controles seleccionados
- Este documento alcanza a las 10 áreas de control del ISO 17799
- Documenta la selección o ausencia de controles, en base a la situación real de la organización.

Aplicando el ISO 17799: paso a paso



La auditoria permite la revisión de la implementación de la infraestructura de seguridad de información.

La auditoria puede ser:

- 1ra parte – Una organización se audita así mismo
- 2da parte – Un cliente o socio realiza la auditoria
- 3ra parte – Un auditor independiente realiza la auditoria

Esta última (3ra parte), es requerida para la Conformidad de la certificación