SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

1.4.0. Capítulo 4
Parte 1 de 2

Plan de implantación de seguridad

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Una vez vista la situación actual, hay que abordar la materialización de las mejoras.

Se analiza con mayor profundidad cuáles son los requisitos deseados de SI para la empresa, y cuáles las condiciones de SI existentes.

La diferencia, el gap o salto de seguridad entre ambas situaciones, es lo que debe corregirse, mediante una implantación de contramedidas que debe ser ordenada, para asegurar la consecución de los objetivos del SGSI.

2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE FRENTE AL NECESARIO

Norma ISO27001

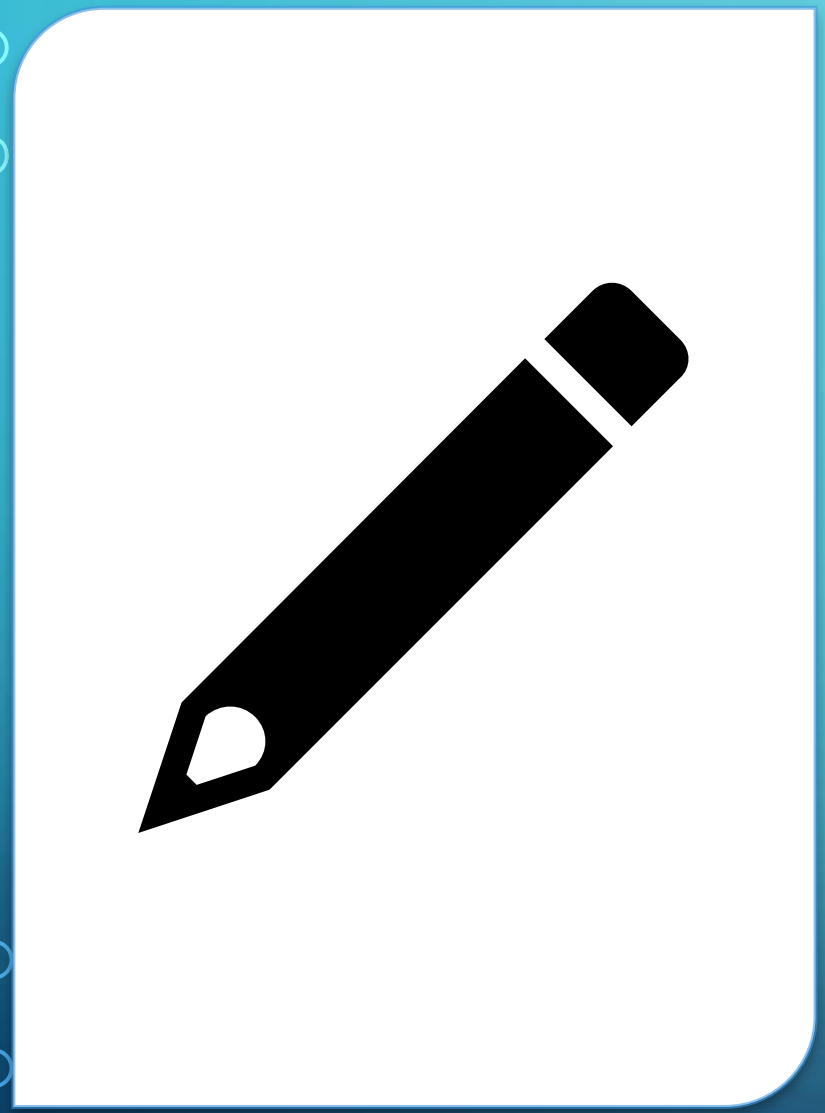
Fase SGSI	Ciclo Deming	Preguntas	Conceptos claves de SI
Establecimiento	Planear	¿Dónde queremos estar?	Requisitos de Seguridad
Implementación y operación	Hacer	¿Cómo llegamos?	Implantación de salvaguardas
Monitorear y revisar	Verificar	¿Dónde estamos? ¿Hemos llegado?	Medida de eficacia de salvaguardas
Mantener y mejorar	Corregir	¿Cómo modificar el rumbo?	Medidas correctivas y lecciones aprendidas

2.1. DETERMINACIÓN DE LOS REQUISITOS DE SEGURIDAD

Según ISO17799:2005, de la que parte ISO 27002 hay tres fuentes principales de requerimientos de seguridad:

- **Evaluación de los riesgos de la organización.**
- **Requisitos legales, reguladores, estatutarios, o por contratos:**
  - **Ley de protección de datos de carácter personal**
  - **Reglamento específico**
  - **ISO 27000**
  - **Código de buenas prácticas del sector.**
- **Conjunto particular de principios, objetivos, y requerimientos comerciales que el sistema de información debe cumplir para sostener las operaciones de la empresa.**

Estos requisitos deben mantenerse actualizados



Actividades

PIENSE EN UN EJEMPLO DE REQUISITOS DE SEGURIDAD PARA LA DISPONIBILIDAD DE LOS SISTEMAS DE UN PROVEEDOR DE HOSTING, BASÁNDOSE EN UNA EVALUACIÓN DE RIESGOS, Y EN LAS PENALIZACIONES ECONÓMICAS SEGÚN EL ACUERDO DE NIVEL DE SERVICIO (SLA, SERVICE LEVEL AGREEMENT), INCLUIDO EN LOS CONTRATOS CON SUS CLIENTES.

2.2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE

¿Dónde estamos?

- **Efectuar revisiones periódicas de la eficacia del SGSI**
- **Medir la efectividad de los controles,**
- **Revisar las evaluaciones de riesgos a intervalos planeados,**
- **Realizar auditorías internas del SGSI a intervalos planeados.**

2.2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE

¿Dónde estamos?

Estudiar y analizar información procedente básicamente de 4 fuentes:

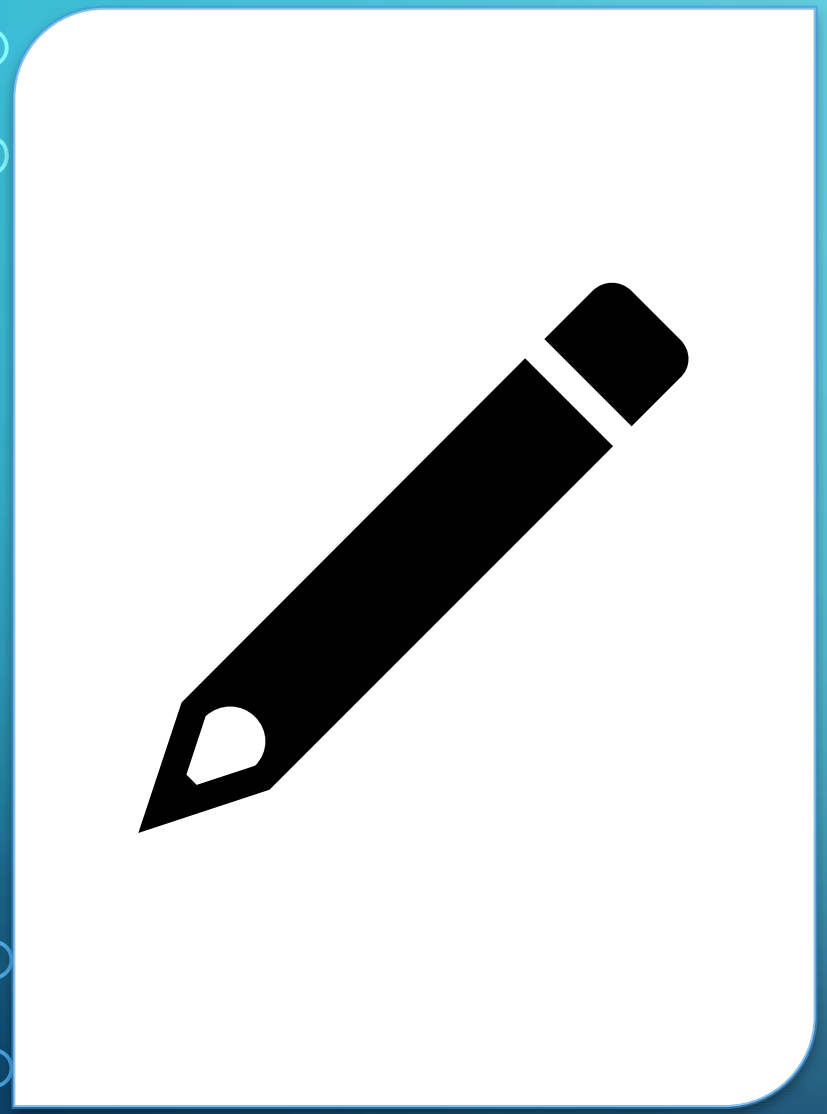
- **Auditorías basadas en riesgo, que implican realizar un AR.**
- **Registros de incidentes de seguridad.**
- **Mediciones de efectividad de las salvaguardas.**
- **Sugerencias y retroalimentación de los interesados.**

2.2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE

¿Dónde estamos?

Ejemplos:

- **Conteo de "no conformidades" en una auditoría ISO 27001.**
- **Conteo de casos en que la operativa de la empresa se aleja de la legislación aplicable.**
- **Conteo del número de casos de incumplimiento de cláusulas de contratos referentes a obligaciones de seguridad de la información.**
- **Conteo del número de casos en que la operación del sistema de información impide el logro de objetivos comerciales de la empresa.**



Actividades

1.4.1.MF0486_3-CAPITULO4_EJEMPLO1.DOCX