

Integrando Calidad y Seguridad



Modelo vs Norma

- ▶ Norma de Calidad: ISO 9001: 2015 - ISO 14001 - ISO 12207
- ▶ Modelos de Calidad: CMMI - ISO 155504 - Modelo Provincial a la Calidad
- ▶ Norma de Seguridad: OHSAS 18001 - ISO 27001/27002
- ▶ Modelo de Seguridad: Modelo de Seguridad de la información (recomendaciones para mantener la confidencialidad, integridad y disponibilidad)

Sistemas de Gestión

- ▶ Que es?
- ▶ Alcance
- ▶ Sistema de gestión integrados (calidad - seguridad - ambiente)
- ▶ Elementos
- ▶ Gestión por procesos: visión del cliente - ciclo de mejora - proveedores.
- ▶ Proceso: entrada - salida - responsable - objetivo.

Circulo de Deming o de mejora continua



Sistema de gestión de seguridad de la información - Etapas

- ▶ Que es un SGSI?
- ▶ Seguridad de la información.
- ▶ Objetivo SGSI: Determinar que se quiere proteger, de quién y cómo lo vamos a proteger.
- ▶ Equivalencia con el ciclo de mejora continua.
 1. Etapa 1: Establecer el SGSI.
 2. Etapa 2: Implementar y operar el SGSI.
 3. Etapa 3 : Monitorear y revisar el SGSI.
 4. Etapa 4: Mantener y mejorar el SGSI.

Gestión de riesgos/prevención/enfoque de riesgos.

- ▶ Es el punto en común en los sistemas de gestión.
- ▶ Para que gestionamos los riesgos?
- ▶ Riesgo: es un evento que puede afectar negativamente los objetivos de una organización.
- ▶ Riesgo de seguridad de la información: Probabilidad de que una amenaza llegue a explotar una vulnerabilidad y genere daños a los activos de una organización.

Pasos de la gestión de riesgos

1. Activos. Ej.
 2. Amenazas. Ej.
 3. Vulnerabilidad. Ej.
 4. Identificación del Riesgos - Ej.
- ▶ Aplicar los 4 pasos en su entorno laboral.

Pasos de la gestión de riesgos

5. Cálculo del riesgo

$$\text{Riesgo} = \text{Impacto} * \text{Probabilidad de ocurrencia}$$

Activo	Amenaza	Impacto	Probabilidad	Riesgo	Prioridad
Página web	Sabotaje	4	0,01	0,04	2
Evaluaciones de desempeño impresas	Inundaciones	3	0,05	0,15	1

Toma de decisiones sobre los riesgos: estrategia de tratamiento.

Controles a implantar para cada riesgo.

Análisis de costo/beneficio.

El problema de la seguridad informática está en su gerenciamiento y no en las tecnologías disponibles.