# 

Investigación

Estudiante:   
Ángela Lemonao  
Módulo o Unidad de Aprendizaje:  
Módulo o Unidad de Aprendizaje  
Fecha: 09-10-2020  
Profesor: Israel Palma

Norma ISO 27001

# Norma ISO 27001

¿Qué es la norma ISO 27001?, Es una norma internacional emitida por la organización internacional de normalización, en la cual se describe como se debe gestionar la seguridad de la información en una empresa. Esta norma, define los factores ambientales de organización (Entornos, información, cultura organizacional), tanto internos como externos, como se planifica, implanta, verifica y controla un sistema de gestión de seguridad de la información. Cualquier empresa puede desplegar un SGSI (Sistema de gestión de la seguridad de la información), puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública.

Es importante considerar que esta norma propone un marco de gestión de la seguridad de toda la información de la empresa, incluso si es información perteneciente al propio conocimiento y experiencia de las personas o la resultante en reuniones, etc.

**Gestión de la calidad PDCA**

La ISO 27001 se basa en la teoría de gestión de la calidad PDCA (también conocida como ciclo de Deming), como se podrá observar en la estructura de esta.

* **Planificar (“Plan”):** etapa inicial de diseño del SGSI en la que se realiza la identificación inicial de los riesgos asociados con la Seguridad de la información. Realizar el análisis de riesgo, define competencias, define las autoridades y las responsabilidades.
* **Hacer (“Do”):** implantación y operación del Sistema de Gestión de Seguridad de la Información definido y desarrollado.
* **Controlar (“Check”):** Revisar y evaluar su eficacia y eficiencia. Si el desempeño no es el esperado analizar las causas y determinar las mejoras. Realiza auditorias del SGSI.
* **Actuar (“Act”):** Adoptar acciones de mejora.

# Fases de un SGSI basado en la norma ISO 27001

En base a este sistema PDCA, la norma ISO 27001 establece las siguientes fases para elaborar un SGSI

1. **Análisis y evaluación de riesgos:** Conocer las principales vulnerabilidades de sus activos de información, se asocian las amenazas relevantes con los activos identificados, identifica el impacto de una perdida de confiabilidad.
2. **Definición de un plan de tratamiento de los riesgos o esquema de mejora:** definir un plan de tratamiento o esquema de mejora, en el que se tengan en cuenta las distintas consecuencias potenciales de esos riesgos, estableciendo una criticidad para cada uno de ellos y así poder evaluar con objetividad las diferentes amenazas.
3. **Alcance de la gestión:** se debe elegir en qué áreas o dependencias de la organización se desea implantar el SGSI como primera medida, cuáles posteriormente y, en algunos casos, determinar si existen ámbitos del negocio que, por sus características, no precisan de la implantación de un protocolo de seguridad.

# Sectores más interesados en la implementación de este sistema

Aunque la norma ISO 27001 es perfectamente válida como guía o base para la implementación de un SGSI en cualquier empresa u organización, con independencia de su tamaño o sector, resulta especialmente interesante, y casi necesaria, en los siguientes sectores:

• Salud.

• Sector público.

• Sector financiero.

## Sector de la salud

La definición y puesta en marcha de un SGSI basado en la norma ISO es especialmente atractiva para las organizaciones médicas, tanto públicas como privadas, por los siguientes motivos:

• La información que manejan es especialmente crítica y confidencial.

• Los requisitos y medidas planteados por la ISO 27001 garantizan la confidencialidad y seguridad de la información de los pacientes y trabajadores ante cualquier amenaza.

• En todo momento se preserva la confidencialidad, integridad y disponibilidad de la información.

• Con la aplicación de este sistema se consiguen ventajas adicionales como:

mejorar la calidad de los servicios, disminuir los tiempos de espera o agilizar

las comunicaciones internas y externas del hospital o centro de salud.

# ¿Puede fallar?

la razón principal por la cual los proyectos de ISO 27001 fallan, es porque la Dirección y/o Administración no proporciona suficientes personas para trabajar en el proyecto o no hay suficientes recursos económicos, el que se tenga el apoyo requerido hay quienes les puede parecer bastante obvio y por lo tanto generalmente no se toma lo suficientemente en serio, por favor, que la labor de concientización y aceptación sea lo más clara posible y asentado en el plan del proyecto.