



ISO 27001,
¿por dónde empezamos?





¿qué es ISO 27001?

La norma ISO/IEC 27001 define los requisitos exigibles a un Sistema de Gestión de la Seguridad de la Información (SGSI) certificable.

¿por qué la información es importante?

Porque es uno de los activos más importantes para una organización.

- ❑ Un uso adecuado de la información permite ofrecer servicios de más valor y, para las empresas, una diferenciación clara frente a la competencia.
- ❑ Un uso inadecuado de la información que no considere la seguridad como un aspecto relevante puede poner en riesgo económico, competitivo o legal a la organización.

¿qué entendemos por seguridad de la información?

La información tiene tres atributos básicos que la caracterizan:

- ❑ Confidencialidad: accesible sólo para quien esté autorizado.
- ❑ Integridad: contenido exacto e inalterado.
- ❑ Disponibilidad: accesible para su uso cuando sea necesario.

La seguridad de la información consiste en la preservación de dichos atributos.



Pero, ¿cuáles son los objetivos de ISO 27001?

1. Incorporar la seguridad dentro de la cultura y el marco de gestión de la organización.
2. Garantizar la confidencialidad, disponibilidad e integridad de la información de la organización para que esta pueda cumplir sus objetivos de negocio, así como los requisitos contractuales y legales existentes.

Y con todo esto, ¿cuáles son sus beneficios?

1. Es una norma certificable que permite demostrar el compromiso con la seguridad de la información frente a terceros.
2. Formaliza la gestión de la seguridad estableciendo una metodología de trabajo sistemática (identificación de activos, análisis de riesgos, etc.).
3. Exige el establecimiento de unos objetivos de seguridad medibles y un criterio de mejora continua para ellos (ciclo de Deming - PDCA).
4. Conciencia a la organización sobre la importancia de la seguridad.
5. Facilita el cumplimiento de requisitos legales y la supervivencia frente a errores, desastres o sabotajes.



Pensemos en unos ejemplos...

- ❑ ¿Cómo se vería afectada la imagen de una organización si su web corporativa fuese alterada de manera no deseada?
- ❑ ¿Cómo se vería afectada una empresa si el ERP donde están los pedidos estuviese fuera de servicio durante varios días?
- ❑ ¿Cómo se vería afectada una empresa si la información de un nuevo producto saliese a la luz antes de tiempo?
- ❑ ¿Cómo se vería afectada una empresa si se inunda el CPD donde se alojan sus servidores?
- ❑ ¿Cómo se vería afectada una empresa si los comerciales no pudiesen acceder al CRM de su intranet cuando están de viaje?
- ❑ ¿Cómo se vería afectada una empresa si un listado con datos personales de los empleados, por ejemplo la nómina, se hiciese público por error?



¿Cómo se implanta un SGSI basado en ISO 27001?

1. Plan - Planificar

- ❑ Definir la política y los objetivos de seguridad
- ❑ Definir el alcance del SGSI
- ❑ Elaborar un inventario de activos y un análisis de riesgos
- ❑ Definir un plan de tratamiento de riesgos que incluya los controles necesarios (partiendo del catálogo establecido en la norma ISO 27002)

2. Do - Hacer

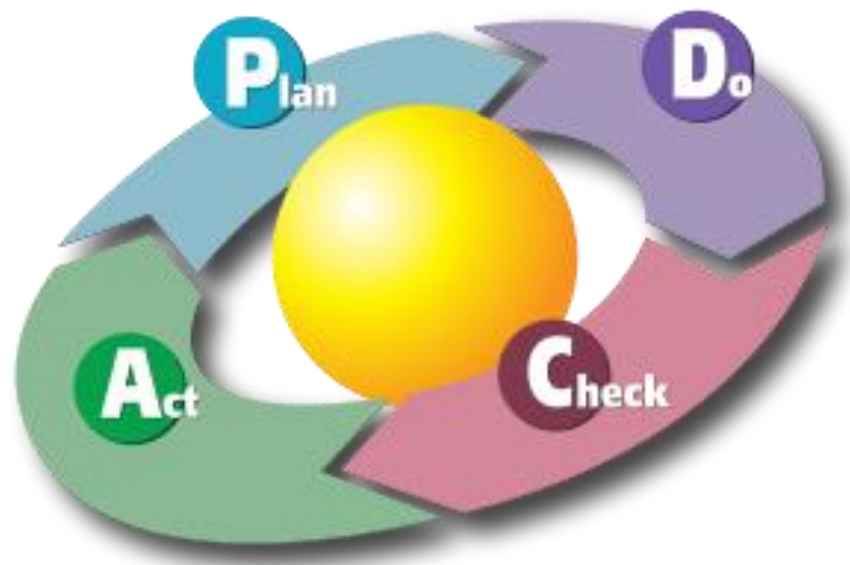
- ❑ Implantar y operar los controles

3. Check - Verificar

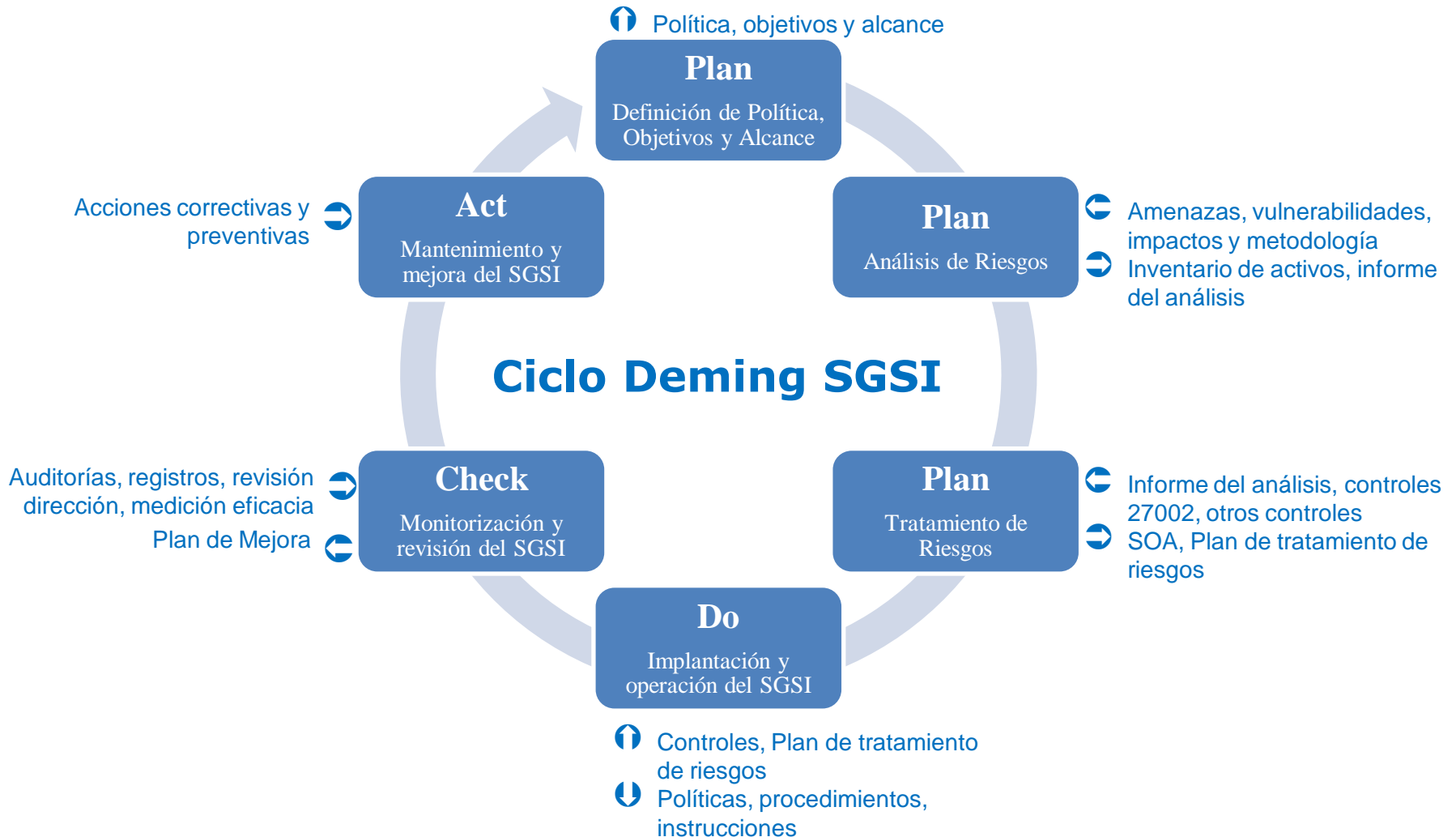
- ❑ Realizar auditorías
- ❑ Medir la eficacia
- ❑ Elaborar un plan de mejora

4. Act - Actuar

- ❑ Ejecutar el plan de mejora



Ciclo de Deming para un SGSI



Estructura de Controles de un SGSI





¿En qué nos ayuda ProactivaNET®?

ProactivaNET® ayuda en la implementación de los controles recogidos en la norma ISO/IEC 27002, que forman el catálogo básico de referencia para la norma ISO/IEC 27001:

- ❑ **ProactivaNET® Service Desk** permite una gestión de las autorizaciones necesarias para la modificación de los recursos de procesamiento de información (A.6.1.4, A.10.1.2, A.12.5.1)
- ❑ **ProactivaNET® CMDB** ayuda a identificar activos (A.7.1.1, A.11.4.3)
- ❑ **ProactivaNET® CMDB** facilita el cálculo de impactos y las dependencias entre activos (A.7.2.1)
- ❑ **ProactivaNET® Service Desk** permite una completa gestión de incidencias de seguridad (A.13.1.1, A.13.2.2, A.13.2.3)
- ❑ **ProactivaNET® Inventario** permite la monitorización y el control de los activos de proceso de información para garantizar su capacidad y un uso adecuado (A.7.1.3, A.10.3.1)
- ❑ **ProactivaNET® Inventario** permite la gestión de los activos entregados al personal o a terceros (A.8.3.2)
- ❑ **ProactivaNET® Inventario** permite la gestión del software instalado y sus licencias (A.9.2.6, A.10.4.1, A.12.4.1)
- ❑ **ProactivaNET® Inventario** permite la revisión de los derechos de acceso de usuarios (A.11.2.4, A.11.6.1)

Trazabilidad normas y estándares

ISO/IEC 20000	ITIL® V2		ITIL® V3	COBIT	ISO/IEC 27002
Gestión de la configuración	Gestión de la configuración	ITIL® V2 Soporte Servicio	Gestión configuración y activos del servicio	DS9 Administrar la configuración	A.12.4.1 Control del software en explotación Activos: A.7.1.1 Inventario A.7.1.2 Propiedad A.8.3.2 Devolución A.9.2.6 Retirada segura
Gestión del cambio	Gestión del cambio		Gestión de cambios	AI6 Administrar cambios	A.10.1.2 Gestión de cambios
Gestión de la entrega	Gestión de la entrega		Gestión de entregas y despliegues Validación y pruebas del servicio Evaluación	AI7 Instalar y acreditar soluciones y cambios	A.10.1.4 Separación de los recursos de desarrollo, prueba y operación A.12 Adquisición, desarrollo y mantenimiento de los SI
Gestión del incidente	Gestión del incidente		Gestión de incidencias Gestión de peticiones	OS8 Administrar la mesa y de servicio y los incidentes	A.13 Gestión de incidentes de seguridad de la información
Gestión del problema	Gestión del problema		Gestión de problemas	DS10 Administración de problemas	A.13.2.2 Aprendizaje de los incidentes de seguridad de la información
Gestión de la capacidad	Gestión de la capacidad		ITIL® V2 Provisión Servicio	Gestión de la capacidad Gestión de la demanda	DS3 Administrar el desempeño y la capacidad
Gestión de la continuidad de servicio de TI y gestión de la disponibilidad	Gestión de la continuidad Gestión de la disponibilidad	Gestión de la disponibilidad Gestión de la continuidad del servicio de TI		DS3 Administrar el desempeño y la capacidad DS4 Garantizar la continuidad del servicio	A.14 Gestión de la continuidad del negocio
Gestión de nivel de servicio Gestión de relaciones con el negocio Gestión de suministradores	Gestión de nivel de servicio	Gestión del nivel de servicio Gestión del catálogo de servicios Gestión de suministradores		DS1 Definir y administrar los niveles de servicio DS2 Administrar los servicios de terceros	A.10.2.1 Provisión de servicios A.10.2.2 Supervisión y revisión de los servicios prestados por terceros
Elaboración de presupuesto y contabilidad para servicios de TI	Gestión financiera	Gestión financiera		PO5 Identificar y asignar costos DS6 Administrar la inversión en TI	
Gestión de la seguridad de la información	Gestión de la seguridad	Gestión de la seguridad de la información		DS5 Garantizar la seguridad de los sistemas	ISO/IEC 27001 ISO/IEC 27002