La norma ISO 27001 del Sistema de Gestión de la

Garantía de confidencialidad, integridad y

Carlos Manuel Fernández
Coordinador de TIC de AENOR

Introducción

La información es como el aparato circulatorio para las organizaciones y requiere que se proteja ante cualquier amenaza que pueda poner en peligro las empresas tanto públicas como privadas, pues en otro caso podría dañarse la salud empresarial.

La realidad nos muestra que las organizaciones empresariales se enfrentan en la actualidad con un alto número de riesgos e inseguridades procedentes de una amplia variedad de fuentes (ver figura 1), entre las que se encuentran los nuevos negocios y nuevas herramientas de las Tecnologías de la Información y la Comunicación (TIC), que los CEO (Directores Generales) y CIO (Directores de Informática) deberían aplicar.

Todas estas herramientas deben aplicarse según objetivos empresariales con la mayor seguridad, garantizando la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (garantizando

Seguridad de la Información

disponibilidad de la información

que la información es fiable y exacta) y disponibilidad (asegurando que los usuarios autorizados tienen el acceso debido a la información).

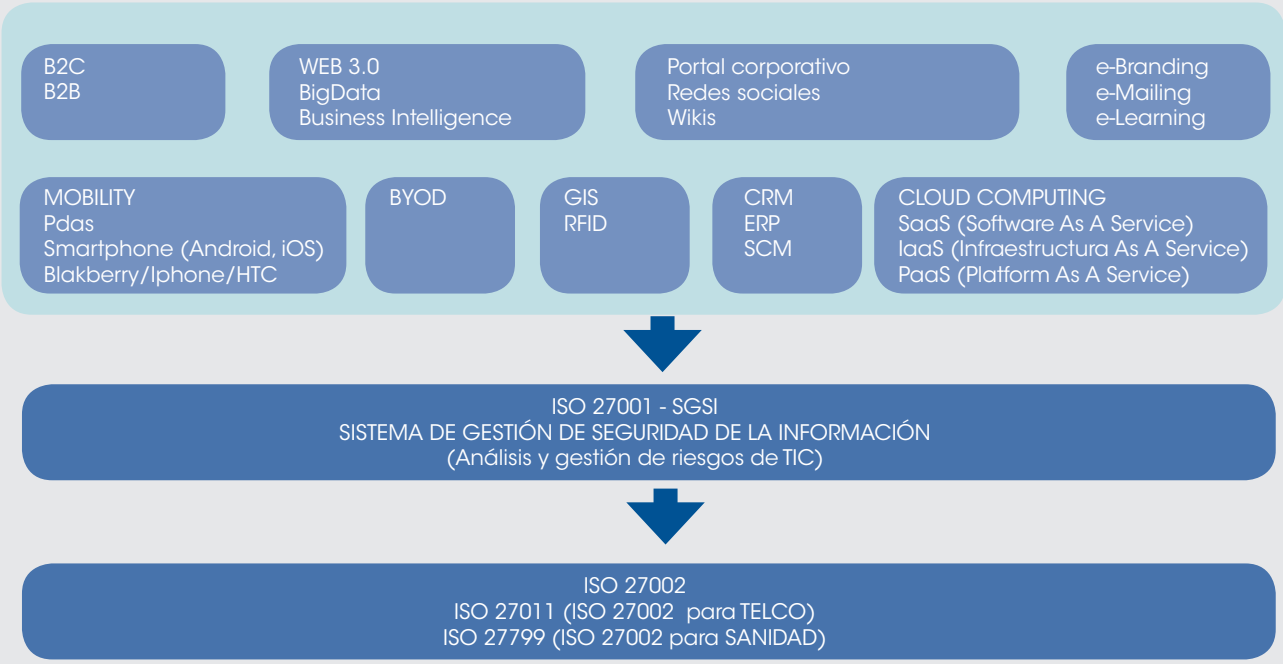
La información, como uno de los principales activos de las organizaciones, debe protegerse a través de la implantación, mantenimiento y mejora de las medidas de seguridad para que cualquier empresa logre sus objetivos de negocio, garantice el cumplimiento legal, de prestigio y de imagen de la compañía.

ISO 27001. Sistema de Gestión de la Seguridad de la Información

La norma/estándar UNE ISO/IEC 27001: 2007 del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles

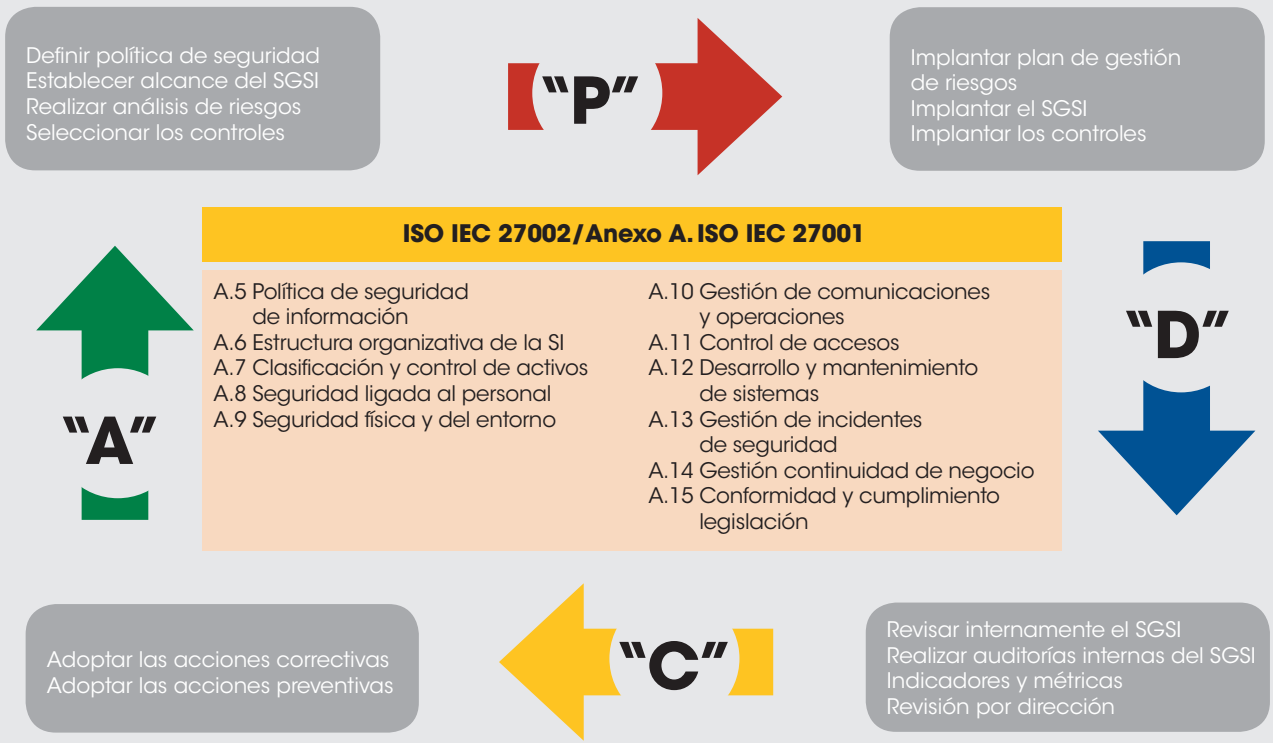
La piedra angular del Sistema de Gestión ISO 27001 es el análisis y gestión de los riesgos basado en los procesos de negocio y servicios de TI

Figura 1. Nuevos negocios y nuevas herramientas en las TIC para los CEO y CIO



Fuente: AENOR.

Figura 2. Sistema de Gestión de la Seguridad de la Información ISO 27001



Fuente: AENOR.

adecuados que aseguren una permanente protección y salvaguarda de la información.

El Sistema de Gestión de la Seguridad de la Información (SGSI) se fundamenta en la norma UNE-ISO/IEC 27001:2007, que sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o de Deming, que consiste en Panificar-Hacer-Verificar-Actuar,más conocido con el acrónimo en inglés PDCA (Plan-DO-Check-Act) (similar a la más extendida y reconocida norma ISO 9001). Asimismo, tiene también su fundamento en la norma UNE–ISO/IEC 27002:2009, que recoge una lista de objetivos de control y controles necesarios para lograr los objetivos de seguridad de la información (ver figura 2).

La piedra angular de este sistema SGSI-ISO 27001 es el análisis y gestión de los riesgos basados en los procesos

España es el segundo país de Europa y el sexto del mundo por número de certificados de Seguridad de la Información, con más de 710 reconocimientos

de negocio/servicios de TI (por ejemplo, CRM, ERP, *Business Inteligence,* redes sociales, movilidad, *cloud computing,* servicios externalizados, *Bring You Own Device,* BYOD, etc.).

El análisis y gestión de los riesgos basado en procesos de negocio/servicios de Tecnologías de Información es una herramienta muy útil para evaluar y controlar una organización con respecto a los riesgos de los sistemas de información. De esta forma los procesos de negocio/servicios de TI se fundamentan en los activos de las TIC que dan soporte a los procesos de negocio/servicios de TI.

Esto exige un análisis y gestión de los riesgos de sistemas de información realista y orientado a los objetivos de la organización. Una vez que se evalúa el riesgo y se aplican los controles adecuados de la UNE ISO/IEC 27002:2009 o de otros estándares nos queda un riesgo residual que la dirección de la empresa aprueba, y que se revisará al menos una vez al año (ver figura 3).

Es de destacar que, como todo sistema de gestión, el SGSI-ISO 27001 tiene además del PDCA unos indicadores (objetivo de la métrica) y métricas para la medición de la eficacia y eficiencia de los controles, que aportan realismo día a día a la seguridad de los SI.

Figura 3. Análisis y gestión de riesgos

Procesos de Negocio / Servicios de TI

Activos de SI

- Sistemas de información (bases de datos)
- *Software*
- *Hardware*
- Telecomunicaciones
- Personas

Análisis y gestión de riesgos

$R = F(\chi_1, \chi_2, \chi_3, \chi_N)$
- Integridad (χ_1)
- Confidencialidad (χ_2)
- Disponibilidad (χ_3)
- Amenazas (χ_4)
- Vulnerabilidades (χ_5)
- Impacto económico (χ_6)
- χ_N

Riesgo residual

$Activo_1$ ----------R'_1
$Activo_2$ ----------R'_2
Aplicando
ISO/IEC 27002
(Selección de controles)

Fuente: AENOR.

Modelo de gobierno y gestión para las TIC

La norma ISO 27001 tiene relación con otras normas que conforman el modelo de gobierno y gestión de las TIC desarrollado por AENOR, basado en estándares aceptados mundialmente (ver figura 4). Se puede decir que, gracias a este modelo, el Centro de Proceso de Datos (CPD) y el resto de la organización comienzan hablar el mismo lenguaje y a interconectarse de manera más natural y eficiente.

Este modelo propone dos certificaciones a máximo nivel: una para el gobierno corporativo de las TIC (según la norma ISO 38500) y otra para el Sistema de Continuidad de Negocio (UNE 71599-2 e ISO 22301) en las empresas. Dentro de la primera divide a su vez la gestión en dos áreas: los Sistemas de Gestión de los Servicios de TI (UNE-ISO/IEC 20000-1) y los Sistemas de Gestión de la Seguridad de la Información (UNE-ISO/IEC 27001). Con la implantación de los sistemas se logra gestionar la calidad y seguridad de los servicios de Tecnologías de Información y Comunicación, lo que trae consigo la minimización de los riesgos en la seguridad de la información y mejorar la seguridad de las TIC en el nivel del servicio de las mismas.

La otra área de gestión es donde se agrupan las actividades de desarrollo de programas *(software),* dirigido a la calidad del proceso de ingeniería del *software,* con el modelo de evaluación, mejora y madurez del *software* (SPICE ISO 15504-ISO 12207).

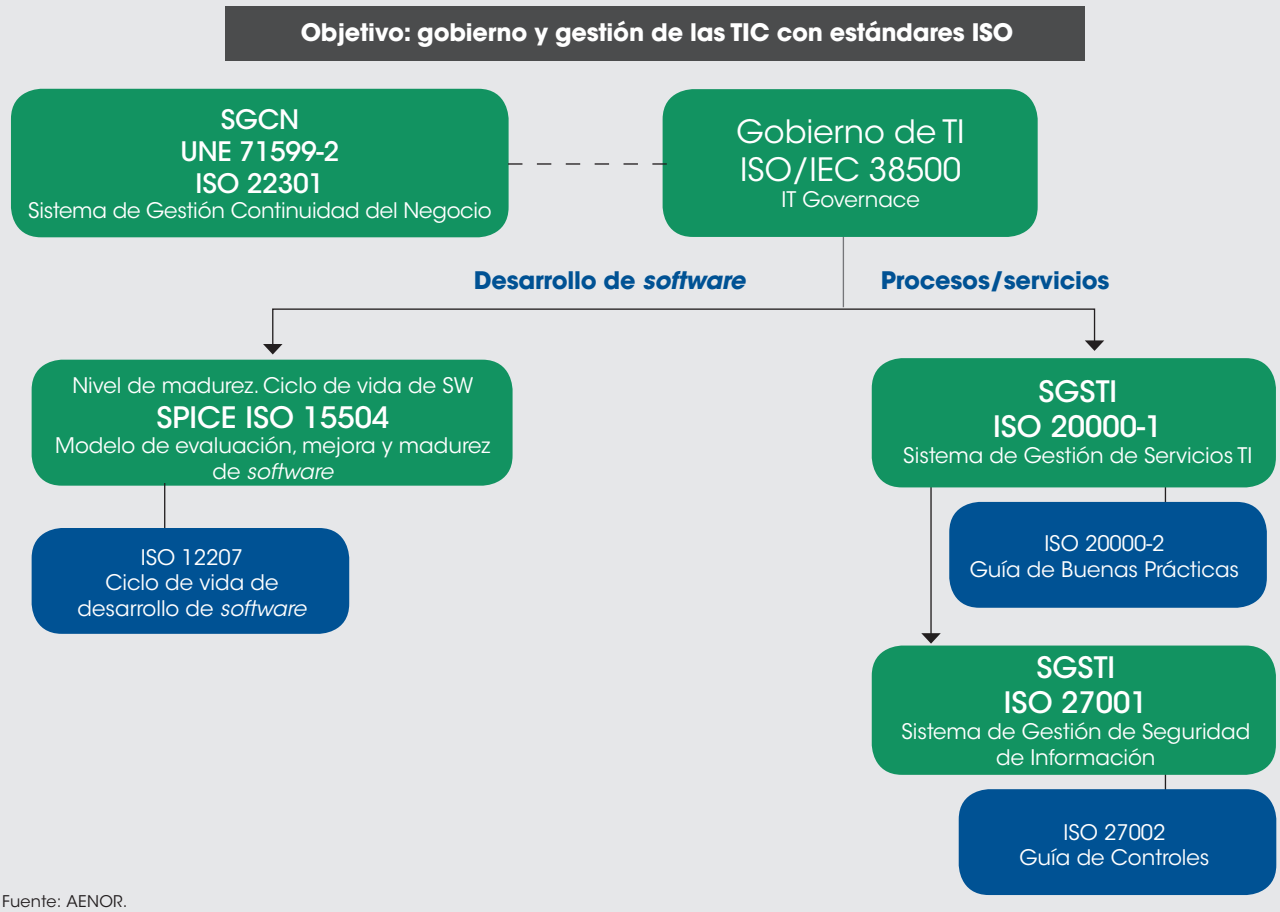
Este modelo significa un cambio cultural que impacta en el mundo empresarial y de las Administraciones Públicas en su relación con las TIC, que ha supuesto el primer paso hacia la consolidación y optimización de las TIC en nuestro país.

Conclusiones

El SGSI-ISO 27001 es un sistema activo, integrado en la organización, orientado a los objetivos empresariales y con una proyección de futuro.

Es importante resaltar que cada vez que se incorpora un nueva herramienta o negocio de TIC a la empresa se debe actualizar el análisis de riesgos para

Figura 4. Modelo de gobierno y gestión de las TIC con normas y estándares ISO



Fuente: AENOR.

poder mitigar de forma responsable los riesgos y, por supuesto, considerando la regla básica de Riesgo de TI *vs.* Control *vs.* Coste, es decir, minimizar los riesgos con medidas de control ajustadas y considerando los costes del control.

Los certificados, por tercera parte independiente, respaldan el cumplimiento de las normas, como en el caso de la ISO 27001. En una economía cada vez más globalizada, en la que los productores españoles de bienes y servicios deben competir, los certificados de conformidad son pasaportes de calidad que abren mercados y una garantía de confianza entre empresas y consumidores de todo el mundo.

En el momento actual, más de 350 organizaciones se han certificado con AENOR en la ISO 27001-SGSI, lo que contribuye a fomentar las actividades de protección de la información en las entidades públicas o privadas, mejorando su seguridad de la información, su imagen y generando confianza frente a terceros. Otros factores intrínsecos al sistema son exponer su voluntad de cumplir con la legislación vigente y garantizar la continuidad del negocio.

Nuestro país ocupa primeros puestos en la clasificación mundial por número de certificados: España es el segundo país de Europa y el sexto del mundo por número de certificados de Seguridad de la Información, con más de 710 reconocimientos, según el último informe de la Organización Internacional de Normalización (ISO).

Este sistema está en plena actualidad y expansión siendo una esplendida herramienta para este siglo XXI, pues supone una salvaguarda continua para los sistemas de información y las nuevas tecnologías. Asimismo supone un referente para otros sistemas como son el Esquema Nacional de Seguridad, los procesos industriales —SCADA—, etc.

Y dado que se trata de un sistema abierto siempre se podrá incorporar cualquier nueva tecnología que irrumpa en el mundo empresarial, por lo que su valor añadido de permanente actualización es un potencial muy a tener en cuenta y a valorar en un mundo tan dinámico y cambiante como lo es el de las TIC. ■