PROCESO DE IMPLEMENTACIÓN DE LOS SISTEMAS DE GESTIÓN ISO 27001 E ISO 22301

DAVID ANDRÉS GONZÁLEZ LEWIS

CISM, CSSLP, PCI QSA, PA QSA, PCIP, ISO27001 IA

C. Santander, 101. Edif. A. 2º
E-08030 Barcelona (Spain)
Tel.: +34 93 305 13 18
Fax: +34 93 278 22 48

C. Arequipa, 1
E-28043 Madrid (Spain)
Tel.: +34 91 763 40 47
Fax: +34 91 382 03 96

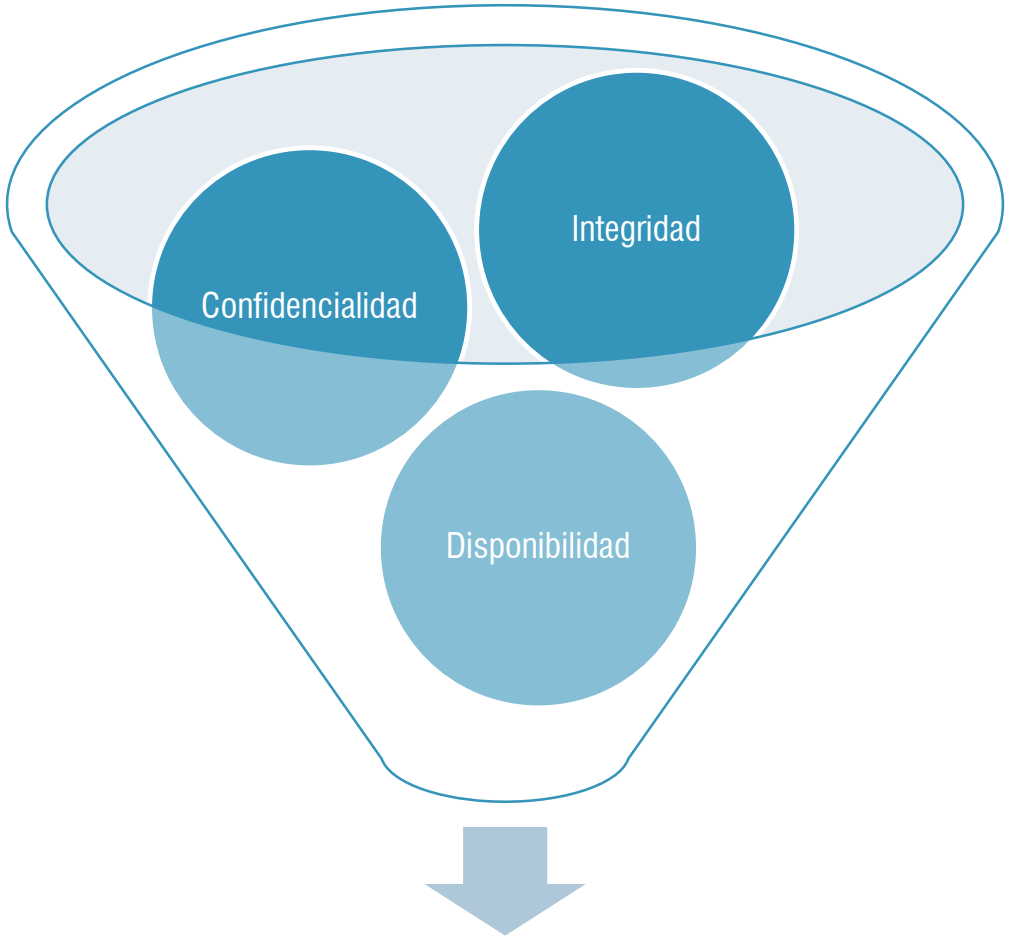
Calle 90 # 12-28
110221 Bogotá (Colombia)
Tel: +57 (1) 638 68 88
Fax: +57 (1) 638 68 88

info@isecauditors.com
www.isecauditors.com

Agenda

- Introducción
- Los sistemas de gestión.
- Implementación ISO 27001
- Implementación ISO 22301
- Mapeo estándares
- Conclusiones

Introducción



Seguridad

Los sistemas de gestión

- **Sistema de Gestión:** Plataforma que permite manejar de forma integrada las actividades para lograr cumplir los objetivos de una organización.

- Anteriormente se trabajaban en forma independiente

- Conjunto de reglas y principios relacionados entre sí de forma ordenada, para contribuir a la **gestión** de procesos generales o específicos de una organización.

- Permite establecer una política, unos objetivos y alcanzar dichos objetivos.

Introducción

ISO 27001:2013

Un Sistema de Gestión de Seguridad de Información (SGSI) es un sistema gerencial general basado en un enfoque de riesgos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

ISO 22301:2012

Proceso continuo de gestión y gobierno, con el apoyo de la alta dirección y con los recursos adecuados para implementar y mantener la gestión de continuidad de las operaciones y/o negocios.

Introducción

¿Qué buscan proteger?

ISO 27001

Proteger la información: la información es considerada un Activo (un recurso) que tiene valor o utilidad para sus operaciones comerciales y su continuidad:

- Activos de Información (datos, manuales de usuario, etc.)
- Documentos en Papel (contratos)
- Activos de software (aplicación, software de sistema, etc.)
- Activos físicos (computadores, medios magnéticos, etc.)
- Personal (clientes, trabajadores)
- Imagen y reputación de la organización
- Servicios (comunicaciones, etc.)

Introducción

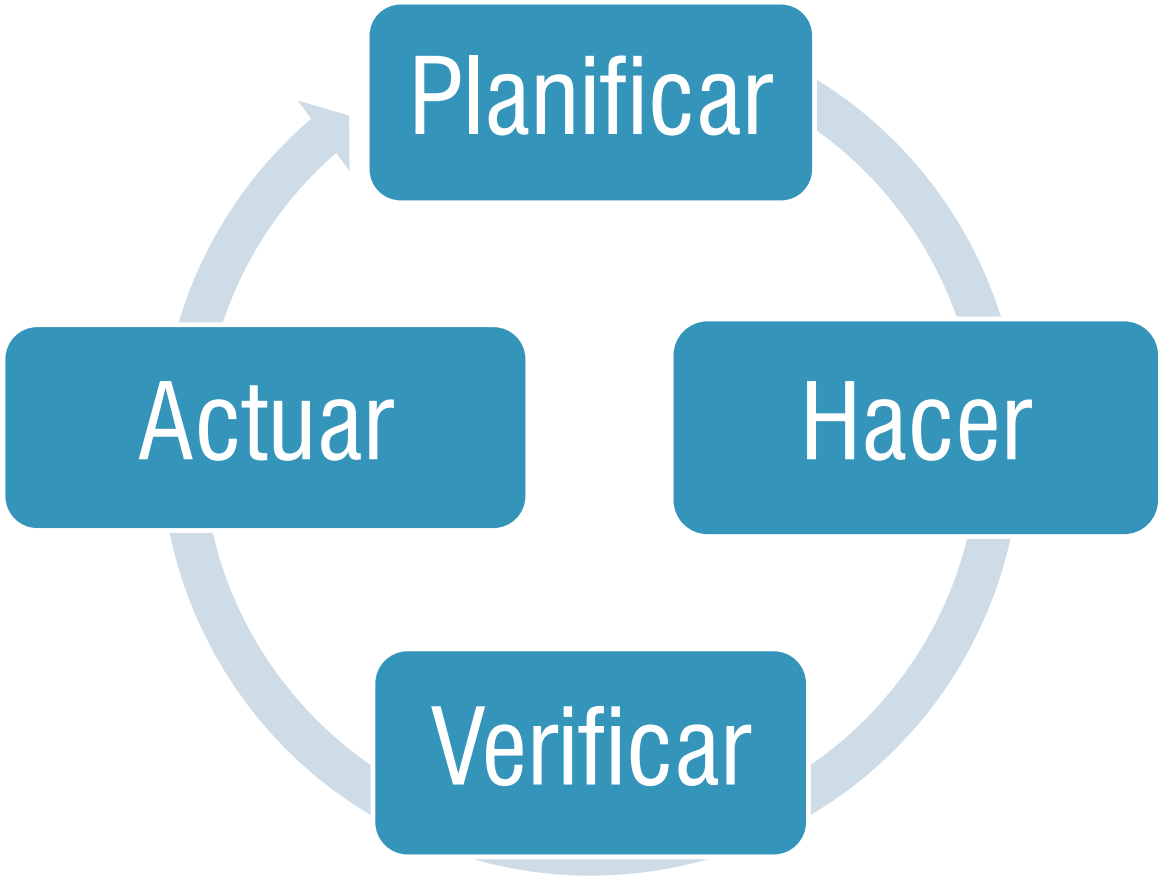
¿Qué buscan proteger?

ISO 22301:2012

Garantizar la continuidad del negocio:

- Asegurar que todos los procesos de negocio críticos estarán disponibles para los clientes, proveedores, y otras entidades que deben acceder a ellos.
- La gestión de la continuidad no se implanta cuando ocurre un desastre, sino que hace referencia a todas aquellas actividades que se llevan a cabo diariamente para mantener el servicio y facilitar la recuperación.

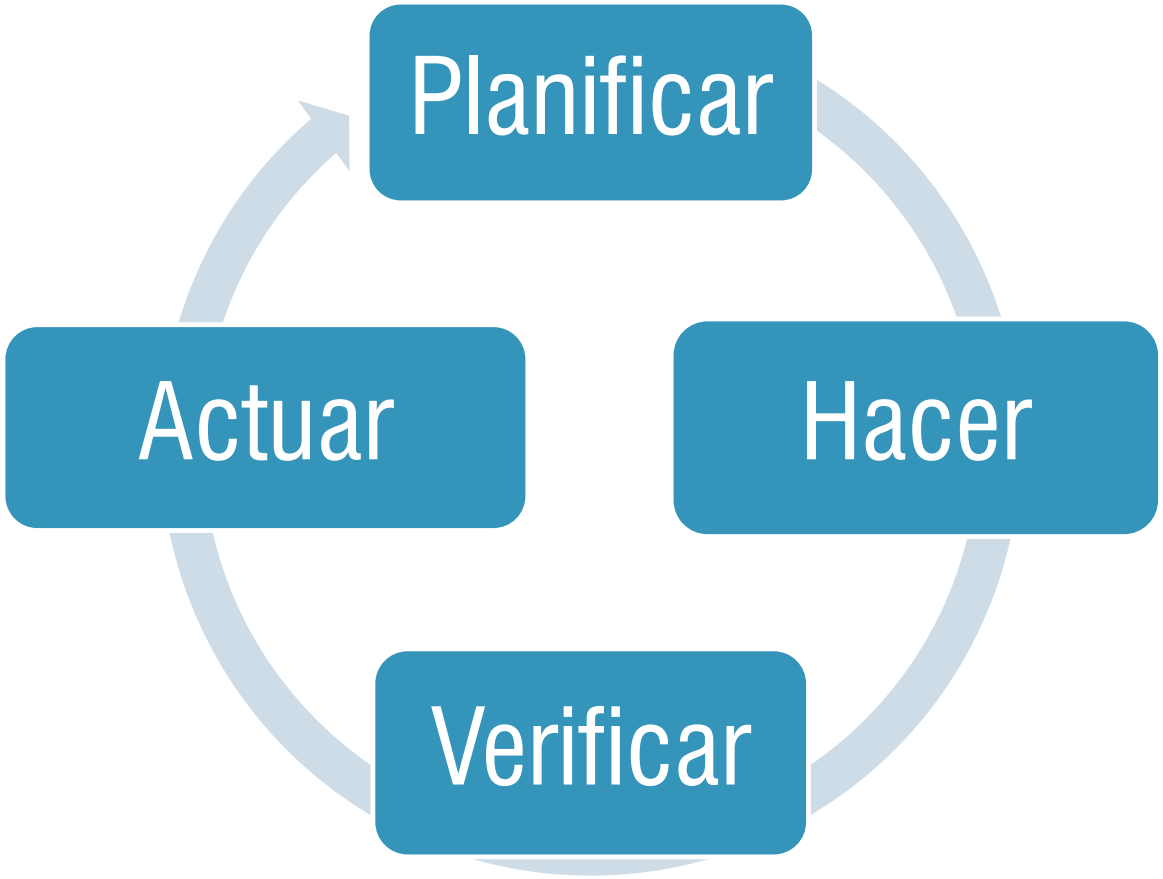
ISO 27001:2013 SGSI



Planear:

- Definir el enfoque de evaluación del riesgo de la organización.
- Identificar los riesgos asociados al alcance establecido.
- Analizar y evaluar los riesgos encontrados.
- Identificar y evaluar las opciones de tratamiento de los riesgos.
- Seleccionar objetivos de control y controles sugeridos por la norma y/u otros que apliquen.
- Obtener la aprobación de la gerencia para los riesgos residuales e implementar el SGSI.
- Preparar el Enunciado de Aplicabilidad.

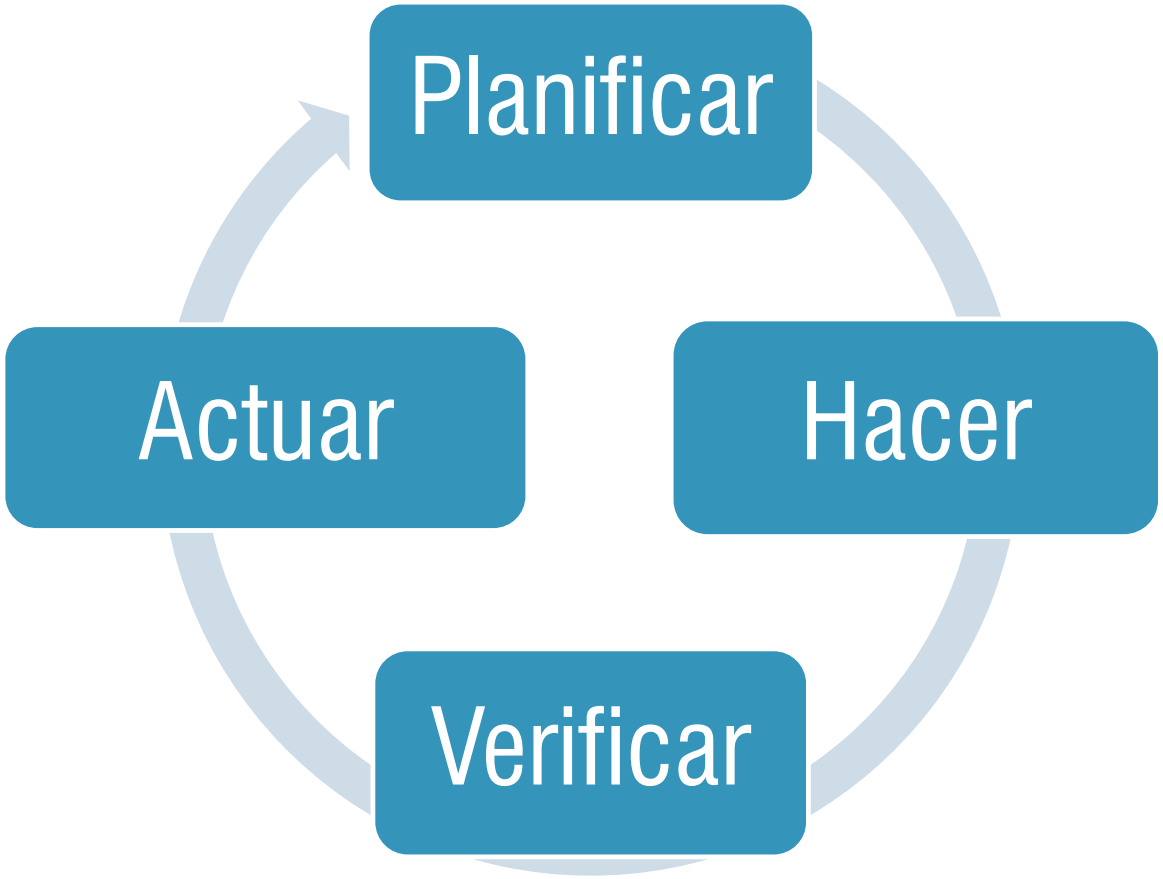
ISO 27001:2013 SGSI



Hacer:

- Plan de tratamiento del riesgo.
- Implementar el plan de tratamiento del riesgo.
- Implementar controles seleccionados.
- Definir la medición de la efectividad de los controles a través de indicadores de gestión.
- Implementar programas de capacitación.
- Manejar las operaciones y recursos del SGSI.
- Implementar procedimientos de detección y respuesta a incidentes de seguridad.

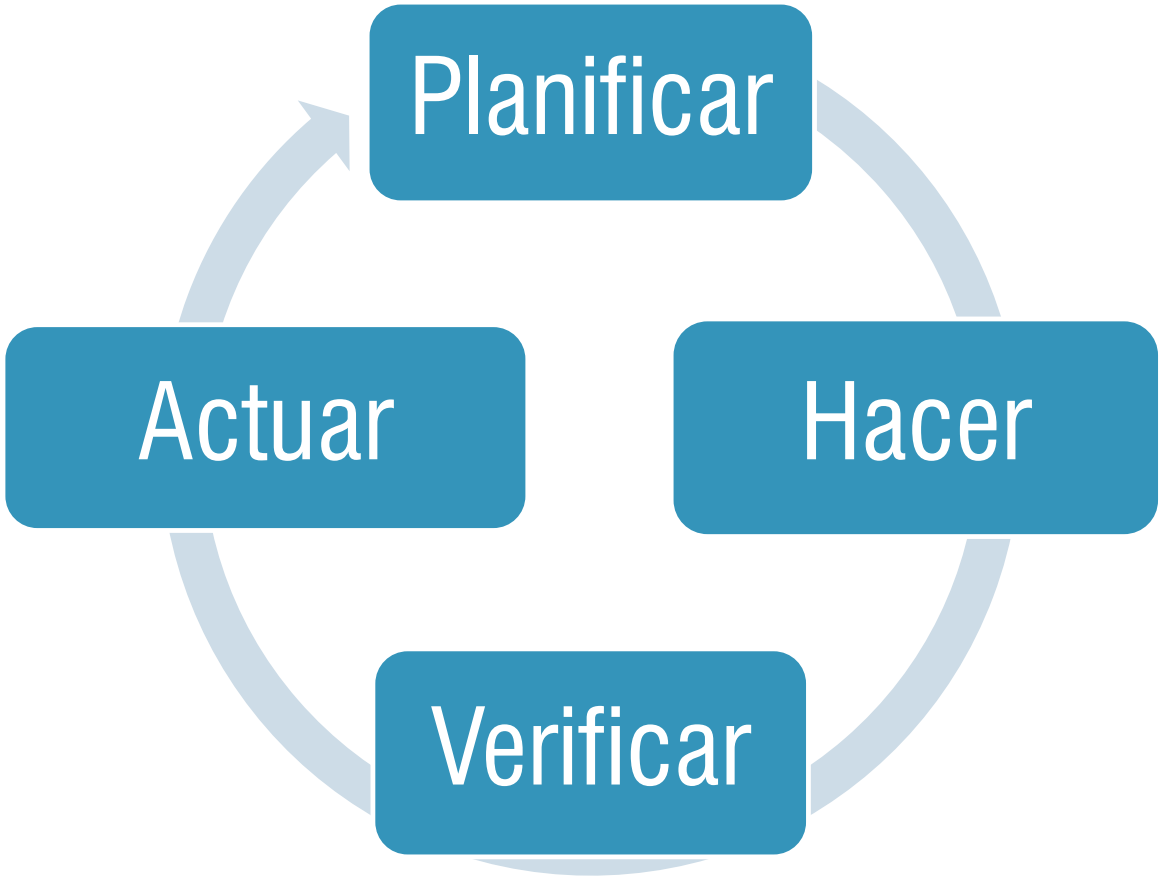
ISO 27001:2013 SGSI



Verificar:

- Procedimientos de monitoreo y revisión para:
  - Detectar oportunamente los errores.
  - Identificar los incidentes y violaciones de seguridad.
  - Determinar la eficacia del SGSI.
  - Detectar eventos de seguridad antes que se conviertan en incidentes de seguridad.
  - Determinar efectividad de las acciones correctivas tomadas para resolver una violación de seguridad.
- Realizar revisiones periódicas.
- Medición de la efectividad de los controles.
- Revisar las evaluaciones del riesgo periódicamente y revisar el nivel de riesgo residual aceptable.
- Realizar auditorías internas al SGSI.
- Realizar revisiones gerenciales.
- Actualizar los planes de seguridad a partir de resultados del monitoreo.

ISO 27001:2013 SGSI



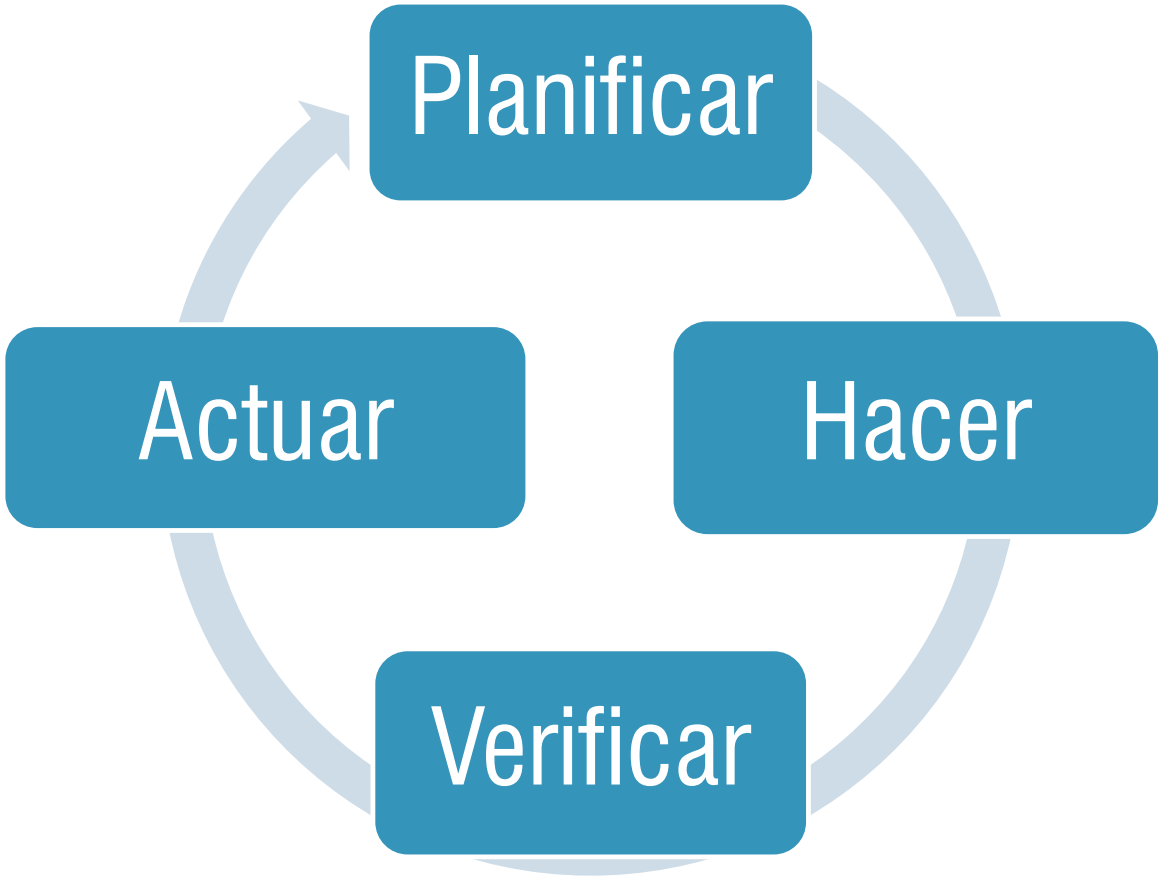
Actuar:

- Implementar las mejoras identificadas en el SGSI.
- Aplicar acciones correctivas y preventivas de seguridad al SGSI.
- Comunicar los resultados y acciones a las partes interesadas.
- Asegurar que las mejoras logren sus objetivos señalados.

ISO 27002:2013 SGSI

Ítem	Nombre
5.	Políticas de Seguridad de la Información
6.	Organización de la seguridad de la información
7.	Seguridad de los recursos humanos
8.	Gestión de activos
9.	Control de acceso
10.	Criptografía
11.	Seguridad física y Ambiental
12.	Seguridad de las Operaciones
13.	Seguridad de las Comunicaciones
14.	Adquisición, desarrollo y mantenimiento de Sistemas
15.	Relaciones con Proveedores
16.	Gestión de incidentes de seguridad de la Información
17.	Aspectos de seguridad de la información en la Gestión de Continuidad de Negocios
18.	Cumplimiento

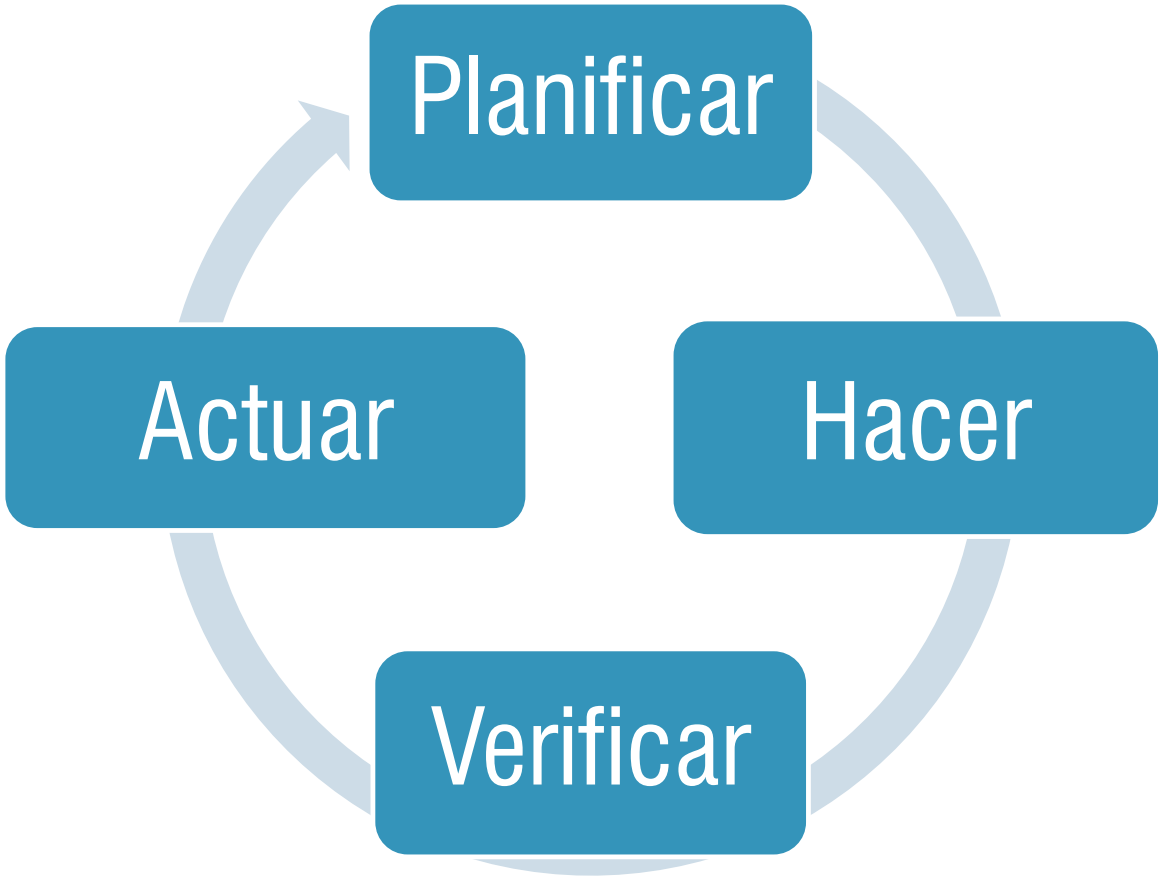
ISO 22301:2012 SGCN



Planificar:

- En este elemento o componente se consideran los principales requisitos dentro del contexto del liderazgo, planeamiento, organización o soporte.
- Establecen objetivos, procesos, procedimientos de continuidad de negocio, para dar alcance los resultados obtenidos, dándole conformidad a los requisitos establecidos por la alta dirección y las políticas de la organización.

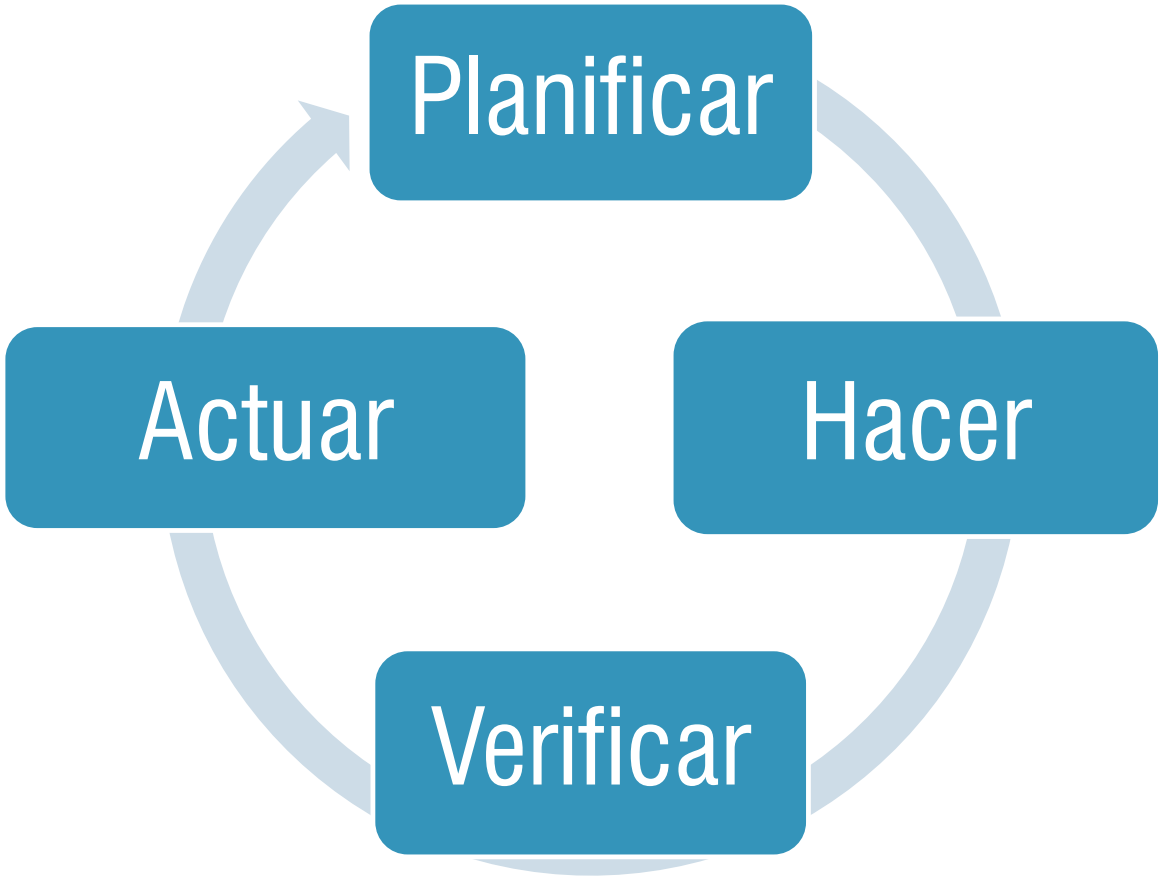
ISO 22301:2012 SGCN



Hacer:

- Fase del proceso integrada por la evaluación de riesgos, proyecto de control y operativo, métodos de continuidad y business impact análisis (BIA).
- Se implementa y pone en marcha los procesos y procedimientos de continuidad de negocio para alcanzar los objetivos.

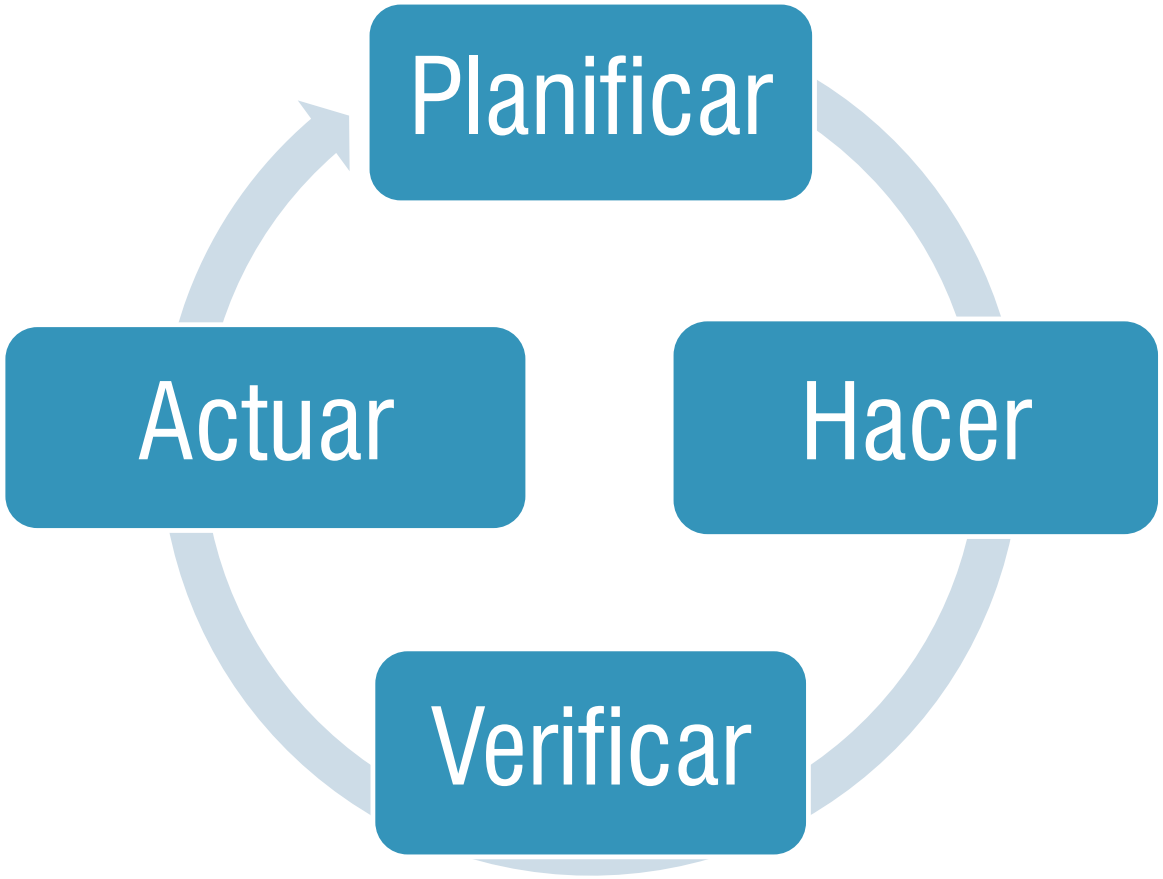
ISO 22301:2012 SGCN



Verificar:

- Fase integrada por el análisis y evaluación, auditoria y revisión, monitoreo y medición.
- Se realiza un seguimiento, a los procesos, conforme a lo establecido en la fase de planificación, reportando los resultados alcanzados, se hacen hallazgos que permiten tomar acciones mejoramiento.

ISO 22301:2012 SGCN



Actuar:

- Fase que abarca los requisitos de acciones de mejoras y/o correctivas y mejora constante.
- Se realizan acciones, para promover la mejora de los procesos, implementando acciones correctivas y volviendo a iniciarse el ciclo con un nuevo plan de mejora.

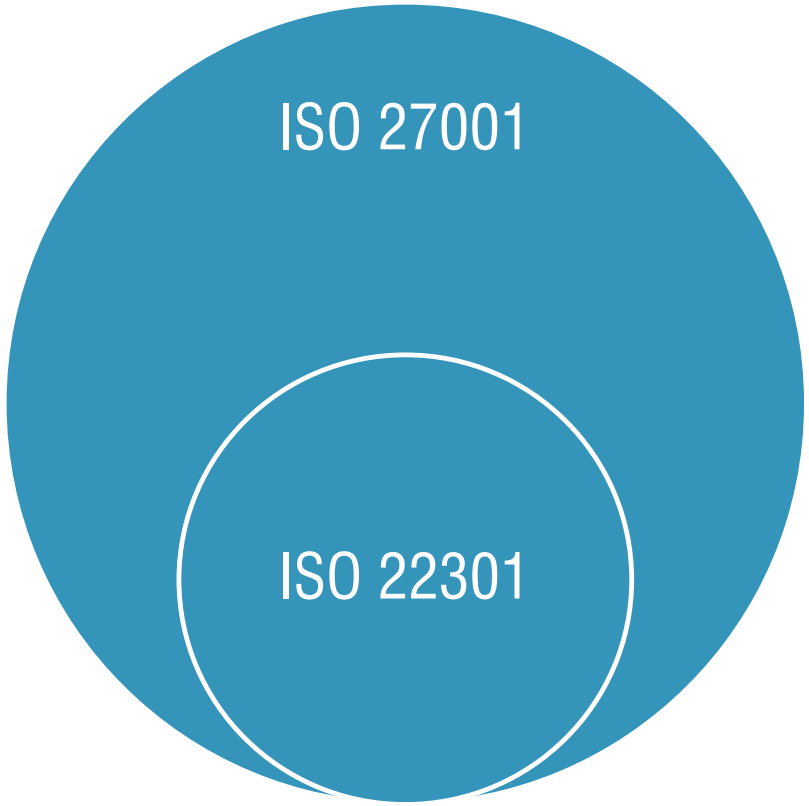
Mapeo Estándares

- **ISO 22301** es totalmente utilizable como **parte de un proceso de certificación de la norma ISO / IEC 27001**.
- Cláusula A.17 – ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO.

ISO 27001 A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO			ISO 22301
A.17.1.1	Planificación de la Continuidad de la seguridad de la Información	***Control*** La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	6 Planificación Sistema de gestión de la Continuidad del Negocio
A.17.1.2	Implementación de la continuidad de la seguridad de la información	***Control*** La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	8.4 Establecimiento e implantación de procedimientos de continuidad del negocio
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	***Control*** La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	8.5 Pruebas y Ensayos
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	***Control*** Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	8.3.2 Establecimiento de los requisitos relativos a los recursos

Mapeo Estándares

- Los controles a implementar en ISO 27002:2013 buscan garantizar la DISPONIBILIDAD de componentes que apoyan la operación, lo cual busca garantizar la continuidad del negocio.
- Las normas:
  - Administración de Documentación
  - Control de Recurso Humando
  - Auditorias Internas
  - Revisiones por la dirección
  - Acciones Correctivas
  - Definición de Objetivos y métricas.



Conclusión

- El sistema de gestión SGSI da una completa gestión de la seguridad y el SGCN es una parte importante de la seguridad de la información.
- Pueden abarcarse la implementación de ambos estándares en una misma aplicación.
- Se pueden utilizar actividades comunes para la implementación de ambos sistemas.
- Los sistemas de gestión permiten dar respuesta a las necesidades de un mercado competitivo y cada vez más exigente, de forma rentable, manteniendo el bienestar laboral y social, controlando los impactos generados de la operación, con base en los lineamientos legales de cada país.

C. Santander, 101. Edif. A. 2º
E-08030 Barcelona (Spain)
Tel.: +34 93 305 13 18
Fax: +34 93 278 22 48

C. Arequipa, 1
E-28043 Madrid (Spain)
Tel.: +34 91 763 40 47
Fax: +34 91 382 03 96

Calle 90 # 12-28. Bogotá
(Colombia)
Tel: +57 (1) 638 68 88
Fax: +57 (1) 638 68 88

info@isecauditors.com
www.isecauditors.com

C. Santander, 101. Edif. A. 2º
E-08030 Barcelona (Spain)
Tel.: +34 93 305 13 18
Fax: +34 93 278 22 48

C. Arequipa, 1
E-28043 Madrid (Spain)
Tel.: +34 91 763 40 47
Fax: +34 91 382 03 96

Calle 90 # 12-28. Bogotá
(Colombia)
Tel: +57 (1) 638 68 88
Fax: +57 (1) 638 68 88

info@isecauditors.com
www.isecauditors.com